EVERY BRAID ADMITS A SHORT SIGMA-DEFINITE REPRESENTATIVE

JEAN FROMENTIN

Abstract. A result by Dehornoy (1992) says that every nontrivial braid admits a σ-definite word representative, defined as a braid word in which the generator σ_i with maximal index i appears with exponents that are all positive, or all negative. This is the ground result for ordering braids. In this paper, we enhance this result and prove that every braid admits a σ-definite word representative that, in addition, is quasi-geodesic. This establishes a longstanding conjecture. Our proof uses the dual braid monoid and a new normal form called the rotating normal form.

It is known since [6] that Artin's braid groups are orderable, by an ordering that enjoys many remarkable properties [11]. The key point in the existence of this ordering is the property that every nontrivial braid admits a σ-definite representative, defined to be a braid word w in the standard Artin generators σ_i in which the generator σ_i with highest index i occurs only positively (no σ_i^{-1}), in which case w is called *σ-positive*, or only negatively (no σ_i), in which case w is called *σ-negative*. For β a braid, let $\|\beta\|_\sigma$ denote the length of the shortest expression of β in terms of the Artin generators $\sigma_1^{\pm1}$. Our main goal in this paper is to prove the following result.

Theorem 1. *Each n-strand braid β admits a σ-definite expression of length at most $6\,(n-1)^2\,\|\beta\|_\sigma$.*

Theorem 1 answers a puzzling open question in the theory of braids. Indeed, the problem of finding a short σ-definite representative word for every braid has an already long history. In the past two decades, at least five or six different proofs of the existence of such σ-definite representatives have been given. The first one by Dehornoy in 1992 relies on self-distributive algebra [6]. The next one, by Larue [18], uses the Artin representation of braids as automorphisms of a free groups, an argument that was independently rediscovered by Fenn–Greene–Rolfsen–Rourke–Wiest [14] in a topological language of so-called curve diagrams. A completely different proof based on the geometry of the Cayley graph of B_n and on Garside's theory appears in [7]. Further methods have been proposed in connection with relaxation algorithms, which are strategies for inductively simplifying some geometric object associated with the considered braid, typically a family of closed curves drawn in a punctured disk. Both the methods of Dynnikov–Wiest in [12] and of Bressaud in [4] lead to σ-definite representatives. However, a frustrating feature of all the above methods is that, when one starts with a braid word w of length ℓ, one obtains in the best case the existence of a σ-definite word w' equivalent to w whose length is bounded above by an exponential in ℓ—in the cases of [18, 14, 7, 12, 4], the original method of [6] is much worse. By contrast, experiments, specially those based on the algorithms derived from [7] and [12], strongly suggested the existence of short σ-definite representatives, making it natural to conjecture that every braid word of length ℓ is equivalent to a σ-definite word of length $O(\ell)$. This is what Theorem 1 establishes. It is fair to mention that the method of [12] proves the existence of "relatively short σ-definite representatives". Indeed, it provides for every length ℓ braid word a σ-definite equivalent word whose length with respect to some conveniently extended alphabet lies in $O(\ell)$. However, when the output word is translated back to the alphabet of Artin's generators σ_i, the only upper bound Dynnikov and Wiest could deduce so far is exponential in ℓ.

The statement of Theorem 1 is essentially optimal. Indeed, it is observed in [11, Chapter XVI] that the length $4(n-2)$ braid word

$$\sigma_{n-1}\sigma_{n-2}^{-2}\ldots\sigma_{2}^{-2e}\sigma_{1}^{2e}\sigma_{2}^{2e}\ldots\sigma_{n-2}^{2}\sigma_{n-1}^{-1},$$

with $e=\pm1$ according to the parity of n, is equivalent to no σ-definite word of length smaller than n^2-n-2. Thus, in any case, the factor $(n-1)^2$ of Theorem 1 could not be possibly replaced with a factor less than $O(n)$.

Our proof of Theorem 1 is effective, and it directly leads to an algorithm that returns, for every n-strand braid β, a distinguished σ-definite word $\underline{\mathrm{NF}}_n(\beta)$ that represents β. Analyzing the complexity of this algorithm leads to

Theorem 2. *There exists an effective algorithm which, for each n-strand braid specified by a word of length ℓ, computes the σ-definite word $\underline{\mathrm{NF}}_n(\beta)$ in $O(\ell^2)$ steps.*

We prove Theorems 1 and 2 using the dual braid monoid B_n^{+*} associated with the Birman–Ko–Lee generators and introducing a new normal form on B_n^{+*}, called the rotating normal form, which is analogous to the alternating normal form of [5] and [10]. The rotating normal form is based on the ϕ_n-splitting operation, a natural way of expressing every n-strand dual braid in terms of a finite sequence of $(n-1)$-strand dual braids.

The principle of the argument is as follows. Given a n-strand braid β, we first express it as a fraction $\delta_n^{-t}\,\beta'$, where δ_n is the Garside element of the monoid B_n^{+*} and β' belongs to B_n^{+*}. If the exponent t happens to be greater than the length of the above-mentioned ϕ_n-splitting of β', then the σ-negative factor δ_n^{-t} wins over the σ-positive factor β', and a σ-negative word representing β can be obtained by an easy direct computation. Otherwise, we determine the rotating normal form w of β' and try to find a σ-positive representative of β by pushing the negative factor δ_n^{-t} to the right through the positive part w. The process is incremental. The problem is that certain special σ-negative words, called dangerous, appear in the process. The key point is that rotating normal words satisfy some syntactic conditions that enable them to neutralize dangerous words. In this way, one finally obtains a word representative of β that contains no σ_{n-1}^{-1}, hence is either σ-positive, or involves no σ_{n-1} at all. An induction on the braid index n then allows one to conclude.

The basic step of the above process consists in switching one dangerous factor and one rotating normal word. This step increases the length by a multiplicative factor 3 at most, and this is the way the length and time upper bounds of Theorems 1 and 2 arise.

In this paper, the braid ordering is not used—in contrary, the existence of the latter can be (re)-deduced from our current results. However, the braid ordering is present behind our approach. What actually explains the existence of our normal form is the connection between the rotating normal form of Section 2 and the restriction of the braid ordering to the dual braid monoid, which is sketched in [15].

The paper is organized as follows. In Section 1, we briefly recall the definition of the dual braid monoids and the properties of these monoids that are needed in the sequel, in particular those connected with the Garside structure. In Section 2, we introduce the rotating normal form, which is our new normal form on B_n^{+*}. In Section 3, we establish syntactic constraints about rotating normal words, namely that every normal word is what we call a ladder. In Section 4, we introduce the notion of a dangerous braid word and define the so-called reversing algorithm, which transforms each word consisting of a dangerous word followed by a ladder into a particular type of σ-definite word called a wall. In Section 5 we compute the complexity of the above reversing algorithm. Finally, we put all pieces together and establish Theorems 1 and 2 in Section 6.

1. Dual braid monoids

Our first ingredient for investigating braids will be the Garside structure of the so-called dual braid monoid B_n^{+*}. Here we recall the needed definitions and results.

1.1. **Birman–Ko–Lee generators.** We recall that Artin's braid group B_n is defined for $n \geqslant 2$ by the presentation

$$\left\langle \sigma_1, \dots, \sigma_{n-1}; \begin{array}{rcll} \sigma_i\sigma_j & = & \sigma_j\sigma_i & \text{for } |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i & = & \sigma_j\sigma_i\sigma_j & \text{for } |i-j| = 1 \end{array} \right\rangle. \tag{1.1}$$

The submonoid of B_n generated by $\{\sigma_1, \dots, \sigma_{n-1}\}$ is denoted by B_n^+, and its elements are called *positive braids*. As is well known, the monoid B_n^+ equipped with Garside's fundamental braid Δ_n has the structure of what is now usually called a Garside monoid [16, 8].

The *dual braid monoid* is another submonoid of B_n. It is generated by a subset of B_n that properly includes $\{\sigma_1, \dots, \sigma_{n-1}\}$, and consists of the so-called *Birman–Ko–Lee generators* introduced in [3].

Definition 1.1. (See Figure 1.) For $1 \leqslant p < q$, we put

$$a_{p,q} = \sigma_p \dots \sigma_{q-2}\, \sigma_{q-1}\, \sigma_{q-2}^{-1} \dots \sigma_p^{-1}. \tag{1.2}$$

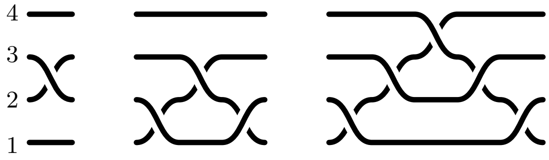

FIGURE 1. From the left to the right : diagram of the braids $a_{2,3}(= \sigma_2)$, $a_{1,3}(= \sigma_1\sigma_2\sigma_1^{-1})$ and $a_{1,4}(= \sigma_1\sigma_2\sigma_3\sigma_2^{-1}\sigma_1^{-1})$. The generator $a_{p,q}$ corresponds to the half-twist where the qth strand crosses over the pth strand, both remaining under all intermediate strands.

Remark 1.2. In [3], $a_{p,q}$ is defined to be $\sigma_{q-1} \dots \sigma_{p+1}\, \sigma_p\, \sigma_{p+1}^{-1} \dots \sigma_{q-1}^{-1}$, *i.e.*, it corresponds to the strands at positions p and q passing in front of all intermediate strands, not behind. Both options lead to isomorphic monoids, but our choice is the only one that naturally leads to the suitable embedding of B_{n-1}^{+*} into B_n^{+*}.

The family of all braids $a_{p,q}$ enjoys nice invariance properties with respect to cyclic permutations of the indices, which are better visualized when $a_{p,q}$ is represented on a cylinder—see Figure 2. Then, it is natural to associate with $a_{p,q}$ the chord connecting the vertices p and q in a circle with n marked vertices [2].

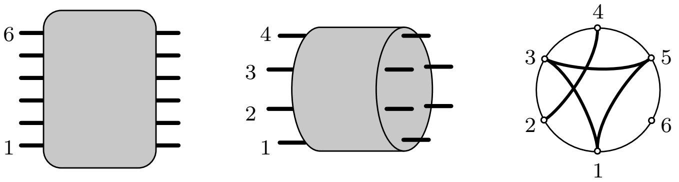

FIGURE 2. Rolling up the usual diagram helps up to visualize the symmetries of the braids $a_{p,q}$. On the resulting cylinder, $a_{p,q}$ naturally corresponds to the chord connecting the vertices p and q.

Hereafter, we write $[p, q]$ for the interval $\{p, \dots, q\}$ of $\mathbb{N}$, and we say that $[p, q]$ is *nested* in $[r, s]$ if we have $r < p < q < s$. A nicely symmetric presentation of B_n in terms of the generators $a_{p,q}$ is as follows.

Lemma 1.3. [3] *In terms of the $a_{p,q}$, the group B_n is presented by the relations*

$$a_{p,q}a_{r,s} = a_{r,s}a_{p,q} \quad \textit{for } [p, q] \textit{ and } [r, s] \textit{ disjoint or nested,} \tag{1.3}$$

$$a_{p,q}a_{q,r} = a_{q,r}a_{p,r} = a_{p,r}a_{p,q} \quad \textit{for } 1 \leqslant p < q < r \leqslant n. \tag{1.4}$$

In the representation of Figure 2, the relations of type (1.3) mean that, in each chord triangle, the product of two adjacent edges taken clockwise does not depend on the edges: for instance, the triangle $(1, 3, 5)$ gives $a_{1,3}a_{3,5} = a_{3,5}a_{1,5} = a_{1,5}a_{1,3}$. Relations of type (1.4) say that the generators associated with non-intersecting chords commute: for instance, on Figure 2, we read that $a_{2,4}$ and $a_{1,5}$ commute—but, for instance, nothing is claimed about $a_{2,4}$ and $a_{1,3}$.

1.2. **The dual braid monoid B_n^{+*} and its Garside structure.** By definition, we have $\sigma_p = a_{p,p+1}$ for each p: every Artin generator is a Birman–Ko–Lee generator. On the other hand, the braid $a_{1,3}$ belongs to no monoid B_n^+. Hence, for $n \geqslant 3$, the submonoid of B_n generated by the Birman–Ko–Lee braids $a_{p,q}$ is a proper extension of B_n^+: this submonoid is what is called the dual braid monoid.

Definition 1.4. For $n \geqslant 2$, the *dual braid monoid* B_n^{+*} is defined to be the submonoid of B_n generated by the braids $a_{p,q}$ with $1 \leqslant p < q \leqslant n$.

So, every positive n-strand braid belongs to B_n^{+*}, but the converse is not true for $n \geqslant 3$: the braid $a_{1,3}$, *i.e.*, $\sigma_1\sigma_2\sigma_1^{-1}$, belongs to B_3^{+*} but not to B_3^+.

Proposition 1.5. [3] *For each n, the relations of Lemma 1.3 make a presentation of B_n^{+*} in terms of the generators $a_{p,q}$, and B_n^{+*} is a Garside monoid with Garside element*

$$\delta_n = a_{1,2}\, a_{2,3} \dots a_{n-1,n} \ (= \sigma_1\, \sigma_2 \dots \sigma_{n-1}). \tag{1.5}$$

Proposition 1.5 implies that the left and right-divisibility relations in the dual braid monoid B_n^{+*} have lattice properties, *i.e.*, that any two elements of B_n^{+*} admit (left and right) greatest common divisors and least common multiples. It also implies that B_n is a group of fractions for the monoid B_n^{+*}, and that every element of B_n^{+*} admits a distinguished decomposition similar to the greedy normal form of B_n^+ [3]. This decomposition involves the so-called simple elements of B_n^{+*}, which are the divisors of δ_n, and are in one-to-one correspondence with the non-crossing partitions of $\{1, ..., n\}$ [3, 1].

1.3. **The rotating automorphism.** An important role in the sequel will be played by the so-called *rotating automorphism* ϕ_n of B_n^{+*}. In every Garside monoid, conjugating under the Garside element defines an automorphism [8]. In the case of the monoid B_n^+ and its Garside element Δ_n, the associated automorphism is the flip automorphism that exchanges σ_i and σ_{n-i} for each i, thus an involution that corresponds to a symmetry in braid diagrams. In the case of the dual monoid B_n^{+*} and its Garside element δ_n, the associated automorphism has order n, and it is similar to a rotation.

Lemma 1.6. *(See Figure 3.) For each β in B_n^{+*}, let $\phi_n(\beta)$ be defined by*

$$\delta_n \beta = \phi_n(\beta) \delta_n. \tag{1.6}$$

Then, for all p, q with $1 \leqslant p < q \leqslant n$, we have

$$\phi_n(a_{p,q}) = \begin{cases} a_{p+1,q+1} & \text{for } q \leqslant n-1, \\ a_{1,p+1} & \text{for } q = n. \end{cases} \tag{1.7}$$

The proof is an easy verification from (1.2), (1.5) and the relations (1.3), (1.4). Note that the relation $\phi_n(a_{p,q}) = a_{p+1,q+1}$ always holds provided the indices are taken mod n and possibly switched so that, for instance, $a_{p+1,n+1}$ means $a_{1,p+1}$.

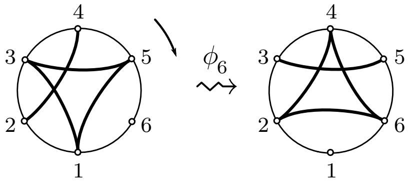

FIGURE 3. Representation of the rotating automorphism ϕ_n as a clockwise rotation of the marked circle by $2\pi/n$.

The formulas of (1.7) show that B_n^{+*} is globally invariant under ϕ_n. By contrast, note that B_n^{+*} is *not* invariant under the flip automorphism Φ_n: for instance, $\Phi_3(a_{1,3})$, which is $\sigma_2\sigma_1\sigma_2^{-1}$, does not belong to B_3^{+*}.

2. The rotating normal form

Besides the Garside structure, the main tool we shall use in this paper is a new normal form for the elements of the dual braid monoid B_n^{+*}, *i.e.*, a new way of associating with every element of B_n^{+*} a distinguished word (in the letters $a_{p,q}$) that represents it. This normal form is called the rotating normal form, as it relies on the rotating automorphism ϕ_n which we have seen is similar to a rotation.

The rotating normal form is reminiscent of the alternating normal form introduced in [10] for the case of the monoid B_n^+—which is itself connected with Burckel's approach of [5]. It is also closely connected with the normal forms introduced in [17], which are other developments, in a different direction, of the alternating normal form. As the properties of B_n^{+*} and ϕ_n are essentially the same as those of B_n^+

and Φ_n, adapting the results of [10] is easy and, therefore, constructing the rotating normal form is not very hard—what will be harder is identifying the needed properties of rotating normal words, as will be done in subsequent sections.

2.1. **The ϕ_n-splitting.** The basic observation of [10] is that each braid in the monoid B_n^+ admits a unique maximal right-divisor that lies in the submonoid B_{n-1}^+. A similar phenomenon occurs in the dual monoid B_n^{+*}.

Lemma 2.1. *For $n \geqslant 3$, every braid β of B_n^{+*} admits a maximal right-divisor lying in B_{n-1}^{+*}. The latter is the unique right-divisor β_1 of β such that $\beta\beta_1^{-1}$ has no nontrivial* (i.e., $\neq 1$) *right-divisor lying in B_{n-1}^{+*}.*

Proof. The submonoid B_{n-1}^{+*} of B_n^{+*} is closed under right-divisor and left-lcm. Hence we can apply Lemma 1.12 of [10]. □

Definition 2.2. The braid β_1 of Lemma 2.1 is called the B_{n-1}^{+*}-*tail* of β and it is denoted by $\mathrm{tail}_{n-1}(\beta)$.

Example 2.3. Let us compute the B_2^{+*}-tail of δ_3^2. As B_2^{+*} is generated by $a_{1,2}$, this B_2^{+*}-tail is the maximal power of $a_{1,2}$ that right-divides δ_3^2. By definition, we have $\delta_3^2 = a_{1,2}a_{2,3}a_{1,2}a_{2,3}$. By applying (1.4) twice, we obtain

$$\delta_3^2 = a_{1,2}a_{2,3}a_{1,3}a_{1,2} = a_{1,2}a_{1,3}a_{1,2}^2.$$

As the word $a_{1,2}a_{1,3}$ is alone in its equivalence class, the braid it represents cannot be right-divisible by $a_{1,2}$. Therefore, the B_2^{+*}-tail of δ_3^2 is $a_{1,2}^2$.

In the context of the monoid B_n^+, one obtains a distinguished decomposition for every braid in B_n^+ by considering the B_{n-1}^+-tail and the $\Phi_n(B_{n-1}^+)$-tail alternatively, which is possible because B_n^+ is generated by B_{n-1}^+ and $\Phi_n(B_{n-1}^+)$. In our context of B_n^{+*}, we shall use the B_{n-1}^{+*}-tail, the $\phi_n(B_{n-1}^{+*})$-tail, ..., the $\phi_n^{n-1}(B_{n-1}^{+*})$-tail cyclically to obtain a distinguished decomposition for every braid of B_n^{+*}.

In order to show that every braid in B_n^{+*} admits such a decomposition, we must check that the images of B_{n-1}^{+*} under the powers of ϕ_n cover B_n^{+*}. Actually, iterating twice is enough.

Lemma 2.4. *For $n \geqslant 3$, every generator $a_{p,q}$ of B_n^{+*} belongs to $B_{n-1}^{+*} \cup \phi_n(B_{n-1}^{+*}) \cup \phi_n^2(B_{n-1}^{+*})$.*

Proof. For $q \leqslant n-1$, the braid $a_{p,q}$ belongs to B_{n-1}^{+*}. Next, for $q = n$ and $p \geqslant 2$, we have $a_{p,n} = \phi_n(a_{p-1,n-1})$, which belongs to $\phi_n(B_{n-1}^{+*})$. Finally, for $p = 1$ and $q = n$, we find $a_{p,q} = \phi_n(a_{n-1,n}) = \phi_n^2(a_{n-2,n-1})$, which belongs to $\phi_n^2(B_{n-1}^{+*})$. □

By iterating the tail construction, we then associate with every braid of B_n^{+*} a finite sequence of braids of B_{n-1}^{+*} that specifies it completely.

Proposition 2.5. *Assume $n \geqslant 3$. Then, for each nontrivial braid β of B_n^{+*}, there exists a unique sequence $(\beta_b, ..., \beta_1)$ in B_{n-1}^{+*} satisfying $\beta_b \neq 1$ and*

$$\beta = \phi_n^{b-1}(\beta_b) \cdot ... \cdot \phi_n(\beta_2) \cdot \beta_1, \tag{2.1}$$

$$\text{for each } k \geqslant 1, \text{ the braid } \beta_k \text{ is the } B_{n-1}^{+*}\text{-tail of } \phi_n^{b-k}(\beta_b) \cdot ... \cdot \beta_k. \tag{2.2}$$

Proof. Starting from $\beta^{(0)} = \beta$, we define two sequences, denoted $\beta^{(k)}$ and β_k, by

$$\beta^{(k)} = \phi_n^{-1}\big(\beta^{(k-1)}\,\beta_k^{-1}\big) \quad \text{and} \quad \beta_k = \mathrm{tail}_{n-1}(\beta^{(k-1)}) \quad \text{for} \quad k \geqslant 1. \tag{2.3}$$

Using induction on $k \geqslant 1$, we prove the relations

$$\beta = \phi_n^k(\beta^{(k)}) \cdot \phi_n^{k-1}(\beta_k) \cdot \ldots \cdot \beta_1, \tag{2.4}$$

$$\mathrm{tail}_{n-1}\big(\phi_n\big(\beta^{(k)}\big)\big) = 1. \tag{2.5}$$

Assume $k = 1$. Lemma 2.1 implies that the B_{n-1}^{+*}-tail of $\beta\,\beta_1^{-1}$ is trivial. Then, as $\phi_n\big(\beta^{(1)}\big)$ is equal to $\beta\,\beta_1^{-1}$, the B_{n-1}^{+*}-tail of $\phi_n\big(\beta^{(1)}\big)$ is trivial, and the relation $\beta = \phi_n(\beta^{(1)}) \cdot \beta_1$ holds. Assume $k \geqslant 2$. By construction of $\beta^{(k)}$, we have $\phi_n(\beta^{(k)}) = \beta^{(k-1)}\,\beta_k^{-1}$, hence $\beta^{(k-1)} = \phi_n(\beta^{(k)}) \cdot \beta_k$. Then we have the relation

$$\phi_n^{k-1}\big(\beta^{(k-1)}\big) = \phi_n^k(\beta^{(k)}) \cdot \phi_n^{k-1}\big(\beta_k\big). \tag{2.6}$$

On the other hand, by induction hypothesis, we have

$$\beta = \phi_n^{k-1}(\beta^{(k-1)}) \cdot \phi_n^{k-2}(\beta_{k-1}) \cdot \ldots \cdot \beta_1. \tag{2.7}$$

Substituting (2.6) in (2.7), we obtain (2.4). As β_k is the B_{n-1}^{+*}-tail of $\beta^{(k-1)}$, Lemma 2.1 gives (2.5).

By construction, the sequence of right-divisors of β,

$$\beta_1,\ \phi_n(\beta_2)\beta_1,\ \phi_n^2(\beta_3)\phi_n(\beta_2)\beta_1,\ \ldots$$

is non-decreasing for divisibility, and, therefore, for length reasons, it must be eventually constant. Hence, by right cancellativity of B_n^{+*}, there exists b such that for $k \geqslant b$, we have $\phi_n^{k-1}(\beta_k) \cdot \ldots \cdot \beta_1 = \phi_n^{b-1}(\beta_b) \cdot \ldots \cdot \beta_1$. Then (2.4) implies

$$\beta = \phi_n^b(\beta^{(b)})\phi_n^{b-1}(\beta_b) \cdot \ldots \cdot \beta_1,$$

with $\beta_b \neq 1$ whenever b is chosen to be minimal.

By definition of b, we have $\beta_k = 1$, and therefore $\phi_n(\beta^{(k)}) = \beta^{(k-1)}$ by (2.3), for $k \geqslant b+1$. Then, we have $\beta^{(b)} = \phi_n(\beta^{(b+1)})$, $\phi_n^{-1}(\beta^{(b)}) = \phi_n(\beta^{(b+2)})$ and $\phi_n^{-2}(\beta^{(b)}) = \phi_n(\beta^{(b+3)})$. By (2.5), the B_{n-1}^{+*}-tails of $\beta^{(b)}$, $\phi_n^{-1}(\beta^{(b)})$ and $\phi_n^{-2}(\beta^{(b)})$ are trivial. Hence, for every generator x of B_{n-1}^{+*}, the braid $\beta^{(b)}$ is not right-divisible by x, nor is it either by $\phi_n(x)$ or by $\phi_n^2(x)$. Then Lemma 2.4 implies that $\beta^{(b)}$ is right-divisible by no $a_{p,q}$ with $1 \leqslant p < q \leqslant n$, *i.e.*, we have $\beta^{(b)} = 1$, whence $\beta = \phi_n^{b-1}(\beta_b) \cdot \ldots \cdot \beta_1$.

We prove now the uniqueness of $(\beta_b, \ldots, \beta_1)$. Let $\phi_n^{c-1}(\gamma_c) \cdot \ldots \cdot \phi_n(\gamma_2) \cdot \phi_n(\gamma_1)$ be a decomposition of β satisfying $\gamma_c \neq 1$ and $\gamma_k = \mathrm{tail}_{n-1}(\phi_n^{c-k}(\gamma_c) \cdot \ldots \cdot \gamma_k)$ for each $k \geqslant 1$. Using an induction on $k \geqslant 1$, we prove the relations

$$\gamma_k = \beta_k \quad \text{and} \quad \phi_n^{c-k-1}(\gamma_c) \cdot \ldots \cdot \phi_n(\gamma_{k+2}) \cdot \gamma_{k+1} = \beta^{(k)}.$$

For $k = 1$, by hypothesis, we have $\beta = \big(\phi_n^{c-1}(\gamma_c) \cdot \ldots \cdot \phi_n(\gamma_2)\big) \cdot \gamma_1$, where γ_1 is the B_{n-1}^{+*}-tail of β, hence, by Lemma 2.1, we have $\beta_1 = \gamma_1$ and $\beta^{(1)} = \phi_n^{c-2}(\gamma_c) \cdot \ldots \cdot \phi_n(\gamma_3) \cdot \gamma_2$. By induction hypothesis, we have

$$\big(\phi_n^{c-k-1}(\gamma_c) \cdot \ldots \cdot \phi_n(\gamma_{k+2})\big) \cdot \gamma_{k+1} = \beta^{(k)},$$

and by hypothesis about γ_{k+1}, the braid γ_{k+1} is the B_{n-1}^{+*}-tail of $\beta^{(k)}$. Then, by Lemma 2.1 again, we have $\gamma_{k+1} = \beta_{k+1}$ and $\phi_n^{c-k-2}(\gamma_c) \cdot \ldots \cdot \phi_n(\gamma_{k+3}) \cdot \gamma_{k+2} = \beta^{(k+1)}$. We proved $\gamma_k = \beta_k$ for $b \geqslant k \geqslant 1$, hence we find

$$\phi_n^{c-b-1}(\gamma_c) \cdot \ldots \cdot \phi_n(\gamma_{b+2}) \cdot \gamma_{b+1} = \beta^{(b)} \tag{2.8}$$

By definition of b, we have $\beta^{(b)} = 1$, whereas, by hypothesis, the braid γ_c is nontrivial. So (2.8) may hold only for $c = b$. □

Definition 2.6. The sequence $(\beta_b, \dots, \beta_1)$ of Proposition 2.5 is called the *ϕ_n-splitting of β*. Its length, *i.e.*, the parameter b, is called the *n-breadth* of β.

The idea of the ϕ_n-splitting is very simple: starting with a braid β of B_n^{+*}, we extract the maximal right-divisor that lies in B_{n-1}^{+*}, *i.e.*, that leaves the nth strand unbraided, then we extract the maximal right-divisor of the remainder that leaves the first strand unbraided, and so on rotating by $2\pi/n$ at each step—see Figure 4.

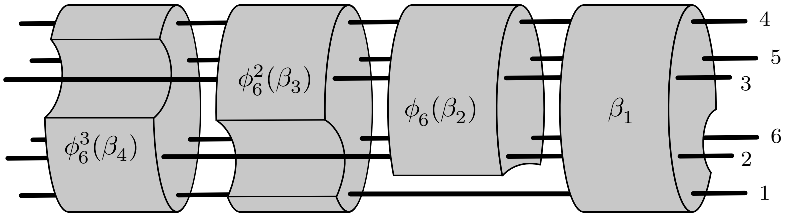

FIGURE 4. The ϕ_6-splitting of a braid of B_6^{+*}. Starting from the right, we extract the maximal right-divisor that keeps the sixth strand unbraided, then rotate by $2\pi/6$ and extract the maximal right-divisor that keeps the first strand unbraided, etc.

In practice, we shall use the following criterion for recognizing a ϕ_n-splitting.

Lemma 2.7. *Condition* (2.2) *is equivalent to*

$$\textit{for each } k \geqslant 1, \textit{ the } B_{n-1}^{+*}\textit{-tail of } \phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_{k+1}) \textit{ is trivial.} \tag{2.9}$$

Proof. By Lemma 2.1, for every $k \geqslant 1$, the braid β_k is the B_{n-1}^{+*}-tail of the braid $\phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_{k+1}) \cdot \beta_k$ if and only if the B_{n-1}^{+*}-tail of $\phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_{k+1})$ is trivial. Hence (2.2) and (2.9) are equivalent. □

As the notion of ϕ_n-splitting is both new and fundamental for the sequel, we mention several examples.

Example 2.8. Let us first determine the ϕ_n-splitting of the Birman–Ko–Lee generators of B_n^{+*}. For $q \leqslant n-1$, the braid $a_{p,q}$ belongs to B_{n-1}^{+*}, then its ϕ_n-splitting is $(a_{p,q})$. As $a_{p,n}$ does not lie in B_{n-1}^{+*}, the rightmost entry in its ϕ_n-splitting must be 1. Now, we have $\phi_n^{-1}(a_{p,n}) = a_{p-1,n-1}$ for $p \geqslant 2$. Hence, for $p \geqslant 2$, the ϕ_n-splitting of $a_{p,n}$ is $(a_{p-1,n-1}, 1)$. Finally, the braids $a_{1,n}$ and $\phi_n^{-1}(a_{1,n}) = a_{n-1,n}$ do not lie in B_{n-1}^{+*}, but $\phi_n^{-2}(a_{1,n}) = a_{n-2,n-1}$ does. So the ϕ_n-splitting of $a_{1,n}$ is $(a_{n-2,n-1}, 1, 1)$. To summarize, the ϕ_n-splitting of $a_{p,q}$ is

$$\begin{cases} (a_{p,q}) & \text{for } p < q \leqslant n-1, \\ (a_{p-1,n-1}, 1) & \text{for } 2 \leqslant p \text{ and } q = n, \\ (a_{n-2,n-1}, 1, 1) & \text{for } p = 1 \text{ and } q = n. \end{cases} \tag{2.10}$$

Example 2.9. Let us compute the ϕ_3-splitting of δ_3^2. With the notation of the proof of Proposition 2.5, we obtain

$$\begin{array}{ll}
\beta^{(0)} = \beta = (a_{1,2}\, a_{2,3})^2 & \beta_1 = \mathrm{tail}_2(\beta^{(0)}) = a_{1,2}^2 \\
\beta^{(1)} = \phi_3^{-1}\big(\beta^{(0)}\beta_1^{-1}\big) = \phi_3^{-1}(a_{1,2}a_{1,3}) = a_{1,3}a_{2,3} & \beta_2 = \mathrm{tail}_2(\beta^{(1)}) = 1 \\
\beta^{(2)} = \phi_3^{-1}\big(\beta^{(1)}\beta_2^{-1}\big) = \phi_3^{-1}(a_{1,3}a_{2,3}) = a_{2,3}a_{1,2} & \beta_3 = \mathrm{tail}_2(\beta^{(2)}) = a_{1,2}, \\
\beta^{(3)} = \phi_3^{-1}\big(\beta^{(2)}\beta_3^{-1}\big) = \phi_3^{-1}(a_{2,3}) = a_{1,2} & \beta_4 = \mathrm{tail}_2(\beta^{(3)}) = a_{1,2}, \\
\beta^{(4)} = \phi_3^{-1}\big(\beta^{(3)}\beta_4^{-1}\big) = 1 &
\end{array}$$

and we stop as the remainder $\beta^{(4)}$ is trivial. Thus the ϕ_3-splitting of δ_3^2 is the sequence $(a_{1,2}, a_{1,2}, 1, a_{1,2}^2)$.

2.2. **The rotating normal form.** Using the ϕ_n-splitting, we shall now construct a unique normal form for the elements of B_n^{+*}, *i.e.*, we identify for each braid β in B_n^{+*} a distinguished word that represents β.

The principle is as follows. First, each braid of B_2^{+*} is represented by a unique word $a_{1,2}^k$. Then, the ϕ_n-splitting provides a distinguished decomposition for every braid of B_n^{+*} in terms of braids of B_{n-1}^{+*}. So, using induction on n, we can define a normal form for β in B_n^{+*} starting with the normal form of the entries in the ϕ_n-splitting of β.

For the rest of this paper, it will be convenient to take the following conventions for braid words and the braids they represent.

Definition 2.10. A word on the letters σ_i (*resp.* on the letters $a_{p,q}$) is called a *σ-word* (*resp.* an *a-word*). The set of all positive n-strand a-words is denoted by $\underline{B}_n^{+*}$. The braid represented by an a-word or a σ-word w is denoted by $\overline{w}$. For w a σ-word or an a-word and w' a σ-word or an a-word, we say that w is equivalent to w', denoted $w \equiv w'$, if we have $\overline{w} = \overline{w'}$.

According to the formulas (1.7), ϕ_n maps each braid $a_{p,q}$ to another similar braid $a_{r,s}$. Using this observation, we can introduce the alphabetical homomorphism, still denoted ϕ_n, that maps the letter $a_{p,q}$ to the corresponding letter $a_{r,s}$, and extends to every a-word. Note that, in this way, if the a-word w represents the braid β, then $\phi_n(w)$ represents $\phi_n(\beta)$.

Definition 2.11. (i) For β in B_2^{+*}, the *ϕ_2-rotating normal form* of β is defined to be the unique a-word $a_{1,2}^k$ that represents β.

(ii) For β in B_n^{+*} with $n \geqslant 3$, the *ϕ_n-rotating normal form* of β is defined to be the a-word $\phi_n^{b-1}(w_b) \ldots w_1$, where $(\beta_b, \ldots, \beta_1)$ is the ϕ_n-splitting of β and w_k is the ϕ_{n-1}-rotating normal form of β_k for each k.

As the ϕ_n-splitting of a braid β lying in B_{n-1}^{+*} is the length 1 sequence (β), the ϕ_n-normal form and the ϕ_{n-1}-normal form of β coincide. Therefore, we can drop the subscript n, and speak of the *rotating normal form*, or, simply, of the *normal form*, of a braid of B_n^{+*}. We naturally say that a positive a-word is *normal* if it is the normal form of the braid its represents.

Example 2.12. Let us compute the normal form of δ_4^2. First, we check the equality $\delta_4^2 = a_{1,2}\, a_{1,4}\, \delta_3^2$. Then, the ϕ_4-splitting of δ_4^2 turns out to be $(a_{2,3}, a_{2,3}, 1, \delta_3^2)$. The ϕ_3-splitting of $a_{2,3}$ is $(a_{1,2}, 1)$, and, therefore, its normal form is $\phi_3(a_{1,2})$, which is $a_{2,3}$. Next, we saw in Example 2.9 that the ϕ_3-splitting of δ_3^2 is $(a_{1,2}, a_{1,2}, 1, a_{1,2}^2)$.

Therefore, its normal form is $\phi_3^3(a_{1,2}) \cdot \phi_3^2(a_{1,2}) \cdot \phi_3(1) \cdot a_{1,2}a_{1,2}$, hence $a_{1,2} \cdot a_{1,3} \cdot \varepsilon \cdot a_{1,2}a_{1,2}$, *i.e.*, $a_{1,2}a_{1,3}a_{1,2}a_{1,2}$. So, finally, the normal form of δ_4^2 is

$$\phi_4^3(a_{2,3}) \cdot \phi_4^2(a_{2,3}) \cdot \phi_4(1) \cdot a_{1,2}a_{1,3}a_{1,2}a_{1,2},$$

hence $a_{1,2} \cdot a_{1,4} \cdot \varepsilon \cdot a_{1,2}a_{1,3}a_{1,2}a_{1,2}$, *i.e.*, $a_{1,2}a_{1,4}a_{1,2}a_{1,3}a_{1,2}a_{1,2}$.

As the relations of Lemma 1.3 preserve the length, positive equivalent a-words always have the same length. Hence, if w' is the unique normal word equivalent to some word w of $\underline{B}_n^{+*}$, then w and w' have the same length.

Proposition 2.13. *For each length ℓ word w of $\underline{B}_n^{+*}$, the normal form of $\overline{w}$ can be computed in at most $O(\ell^2)$ elementary steps.*

Proof. Computing the B_{n-1}^{+*}-tail of the braid $\overline{w}$ can be done in $O(\ell)$ steps. Hence computing the ϕ_n-splitting can be done in $O(\ell^2)$ steps. Taking into account the observation that the lengths of equivalent words are equal, one deduces using an easy induction on n that computing the rotating normal form of $\overline{w}$ can be done in $O(\ell^2)$ steps. □

We considered above the question of going from w to an equivalent normal word, thus first identifying the ϕ_n-splitting of w and then finding the normal form of the successive entries. Conversely, when we start with a normal word w, it is easy to isolate the successive entries of the ϕ_n-splitting of the braid $\overline{w}$, *i.e.*, to group the successive letters in blocks.

Hereafter, if w is a n-normal word , the (unique) sequence of $n-1$-normal words of $(w_b, \dots, w_1)$ such that $(\overline{w_b}, \dots, \overline{w_1})$ is the ϕ_n-splitting of $\overline{w}$ is naturally called the ϕ_n*-splitting* of w.

Lemma 2.14. *Assume $n \geqslant 3$. For each normal word w of $\underline{B}_n^{+*}$, the ϕ_n-splitting of w can be computed in at most $O(\ell)$ elementary steps.*

Proof. By definition of ϕ_n, a generator $a_{p,q}$ lies in $\phi_n^k(B_{n-1}^{+*})$ if and only if we have $p \neq k \mod n$ and $q \neq k \mod n$. Therefore, given a normal word w in $\underline{B}_n^{+*}$, we can directly read the ϕ_n-splitting $(w_b, \dots, w_1)$ of w. Indeed, reading w from the right, w_1 is the maximal suffix of w that lies in $\underline{B}_{n-1}^{+*}$, then $\phi_n(w_2)$ is the maximal suffix of the remaining braid lying in $\phi_n(B_{n-1}^{+*})$, etc, until the empty word is left. □

Example 2.15. Let us consider the normal word $w = a_{1,2}\, a_{1,4}\, a_{2,3}\, a_{1,2}$ and compute the ϕ_4-splitting of w. Reading w form the right, we find that the maximal suffix of w containing no letter $a_{p,q}$ with $p = 0 \mod n$ or $q = 0 \mod n$ is $a_{2,3}\, a_{1,2}$. The latter is the maximal suffix of w lying in $\underline{B}_3^{+*}$, so we have $w_1 = a_{2,3}\, a_{1,2}$. Repeating this process, one would easily find that the ϕ_4-splitting of w is $(\phi_4^{-3}(a_{1,2}),\, \phi_4^{-2}(a_{1,4}),\, \phi_4^{-1}(1),\, a_{2,3}\, a_{1,2})$, hence the sequence $(a_{2,3}, a_{2,3}, 1, a_{2,3}\, a_{1,2})$.

3. Ladders

The ϕ_n-splitting operation associates with every braid in B_n^{+*} a finite sequence of braids in B_{n-1}^{+*}. Now, in the other direction, every sequence of braids in B_{n-1}^{+*} need not be the ϕ_n-splitting of a braid in B_n^{+*}. The aim of this section is to establish constraints that are satisfied by the entries of a ϕ_n-splitting. The main constraint is that a ϕ_n-splitting necessarily contains what we call ladders, which are sequences of (non-adjacent) letters $a_{p,q}$ whose indices q make an increasing sequence (the bars of the ladder).

3.1. **Last letters.** We begin with some elementary observations about the last letters of the normal forms of the entries in a ϕ_n-splitting.

Definition 3.1. For each nonempty word w, the last letter of w is denoted by $w^{\#}$. Then, for each nontrivial braid β in B_n^{+*}, we define the *last letter* of β, denoted $\beta^{\#}$, to be the last letter in the normal form of β.

Lemma 3.2. *Assume $n \geqslant 3$, and let $(\beta_b, \dots, \beta_1)$ be a ϕ_n-splitting.*

(i) For $k \geqslant 2$, the letter $\beta_k^{\#}$ is $a_{p,n-1}$ for some p, unless $\beta_k = 1$ holds.

(ii) For $k \geqslant 3$, we have $\beta_k \neq 1$.

(iii) For $k \geqslant 2$, if the normal form of β_k is $w\, a_{n-2,n-1}$ with w nonempty, then the letter $w^{\#}$ is $a_{p,n-1}$ for some p.

Proof. (i) Assume $k \geqslant 2$. Put $a_{p,q} = \beta_k^{\#}$. By (2.9), the B_{n-1}^{+*}-tail of $\phi_n^{b-k+1}(\beta_b) \cdot \dots \cdot \phi_n(\beta_k)$ is trivial. In particular, $\phi_n(\beta_k^{\#})$ cannot lie in B_{n-1}^{+*}, so $\beta_k^{\#}$ must be a letter of the form $a_{p,n-1}$.

(ii) Assume that we have $\beta_c = 1$ with $c \geqslant 3$ and $\beta_k \neq 1$ for $b \geqslant k > c$. By definition of a ϕ_n-splitting, $\beta_b \neq 1$ holds, hence we must have $c \leqslant b-1$. By definition of c, we have $\beta_{c+1} \neq 1$, hence, by (i), $\beta_{c+1}^{\#} = a_{r,n-1}$ for some r. By (2.9), the B_{n-1}^{+*}-tail of $\phi_n^{b-c-1}(\beta_b) \cdot \dots \cdot \phi_n^2(\beta_{c+1})\, \phi_n(\beta_c)$ is 1. As we have $\beta_c = 1$, we deduce that the B_{n-1}^{+*}-tail of $\phi_n^{b-c-1}(\beta_b) \cdot \dots \cdot \phi_n^2(\beta_{c+1})$ is 1 as well. This implies that the last letter of $\phi_n^2(\beta_{c+1})$, which is $\phi_n^2(a_{r,n-1})$, does not belong to B_{n-1}^{+*}. Then (1.7) implies $r = n-2$ and $\phi_n^3(a_{r,n-1}) = a_{1,2}$. As the normal form of β_{c-1} is a word of $\underline{B}_{n-1}^{+*}$, the braid $\phi_n(\beta_{c-1})$ is represented by a word that contains no letter $a_{1,q}$. Now the relations

$$a_{1,2}\, a_{p,q} \equiv \begin{cases} a_{p,q}\, a_{1,2} & \text{for } 2 < p, \\ a_{1,q}\, a_{1,2} & \text{for } 2 = p, \end{cases}$$

imply that there exists a braid β' in B_n^{+*} satisfying $a_{1,2}\, \phi_n(\beta_{c-1}) \equiv \beta'\, a_{1,2}$. Therefore $a_{1,2}$ is a right-divisor of $\phi_n^3(\beta_{c+1}) \cdot \phi_n^2(\beta_c) \cdot \phi_n(\beta_{c-1})$. As we have $c-1 \geqslant 2$ by hypothesis, this contradicts (2.9).

(iii) Assume that the normal form of β_k is $w\, a_{n-2,n-1}$ with $w \neq \varepsilon$. Let $a_{p,q}$ be the last letter of w. As we have

$$a_{p,q}\, a_{n-2,n-1} \equiv \begin{cases} a_{n-2,n-1}\, a_{p,q} & \text{for } q < n-2, \\ a_{p,n-1}\, a_{p,q} & \text{for } q = n-2, \end{cases} \tag{3.1}$$

we must have $q = n-1$. Indeed, otherwise, $a_{p,q}$ would be a right-divisor of β_k, *i.e.*, the B_{n-1}^{+*}-tail of $\phi_n(\beta_k)$ would be nontrivial, contradicting (2.9). □

3.2. **Barriers.** If $(\beta_b, \dots, \beta_1)$ is the ϕ_n-splitting of a braid of B_n^{+*}, then Lemma 3.2 says that, for $k \geqslant 3$, the letter $\beta_k^{\#}$ must be some letter $a_{p-1,n-1}$. We shall see now that the braid β_{k-1} cannot be an arbitrary braid of B_{n-1}^{+*}: its normal form has to satisfy some constraints involving the integer p, namely to contain a letter called an $a_{p,n}$-barrier—a key point in subsequent results.

Definition 3.3. The letter $a_{r,s}$ is called an *$a_{p,n}$-barrier* if we have

$$1 \leqslant r < p < s \leqslant n-1. \tag{3.2}$$

There exists no $a_{p,n}$-barrier with $n \leqslant 3$; the only $a_{p,4}$-barrier is $a_{1,3}$, which is an $a_{2,4}$-barrier.

By definition, if the letter x is an $a_{p,n}$-barrier, then there exists in the presentation of B_n^{+*} no relation of the form $a_{p,n} \cdot x = y \cdot a_{p,n}$ allowing one to push the letter $a_{p,n}$ to the right through the letter x: so, in some sense, x acts as a barrier. We shall prove now that (almost) every non-terminal entry β_k of a splitting necessarily contains a barrier—a key point for the sequel. The reason is simple: if there were no barrier in β_k, then the relations would enable one to push the last letter of $\phi_n^2(\beta_{k+1})$ through $\phi_n(\beta_k)$ and incorporate it in β_{k-1}, contradicting the definition of a splitting.

Lemma 3.4. *Assume $n \geqslant 3$, that β is a braid of B_{n-1}^{+*} and that the B_{n-1}^{+*}-tail of $\phi_n(a_{p,n}\beta)$ is trivial for $p \leqslant n-2$. Then the normal form of β is not the empty word and it contains an $a_{p,n}$-barrier.*

Proof. We assume that the normal form w of β contains no $a_{p,n}$-barrier, and derive a contradiction. Let w' be the word $a_{p,n}w$ and let X be the set of all letters $a_{q,r}$ with $p < r \leqslant n-1$. Write $w' = u\,v$ where v is the maximal suffix of w containing letters from X only. By hypothesis, the B_{n-1}^{+*}-tail of $\overline{w'}$ is trivial. Hence the word w' ends with $a_{q,n-1}$ for some q, *i.e.*, v is not empty. As the first letter of w' is $a_{p,n}$, which is not in X, the word u is not empty. Let $a_{s,t}$ be the last letter of u. By construction of u, the letter $a_{s,t}$ is either $a_{p,n}$ or it satisfies $t \leqslant p$. In both cases, the braid $\phi_n(a_{s,t})$ lies in B_{n-1}^{+*}. We shall now prove that $a_{s,t}$ quasi-commutes with v, *i.e.*, there exists a word v' satisfying $a_{s,t}v \equiv v'a_{s,t}$. Every letter $a_{q,r}$ occurring in v is not an $a_{p,n}$-barrier, *i.e.*, it satisfies $p \leqslant q < r \leqslant n-1$. Hence, by the relations

$$a_{s,t}a_{q,r} \equiv \begin{cases} a_{q,r}a_{s,t}, & \text{for } p < q \text{ or } t < p \qquad \text{by (1.3)},\\ a_{s,r}a_{s,t}, & \text{for } q = t = p \qquad \text{by (1.4)},\\ a_{r,t}a_{s,t}, & \text{for } q = s = p \qquad \text{by (1.4)}, \end{cases}$$

the letter $a_{s,t}$ quasi-commutes with v. Then, $\phi_n(a_{s,t})$ is a right-divisor of $\phi_n(a_{p,n}\,\beta)$. This contradicts the hypothesis that the B_{n-1}^{+*}-tail of $\phi_n(a_{p,n}\beta)$ is trivial since the braid $\phi_n(a_{s,t})$ belongs to B_{n-1}^{+*}. □

We now show how Lemma 3.4 can be used in the context of a ϕ_n-splitting.

Lemma 3.5. *Let $(\beta_b, \dots, \beta_1)$ be a ϕ_n-splitting of some braid of B_n^{+*} with $n \geqslant 3$. Then, for each k in $\{b-1, \dots, 2\}$ such that $\beta_{k+1}^{\#}$ is not $a_{n-2,n-1}$ (if any), the normal form of β_k contains an $\phi_n(\beta_{k+1}^{\#})$-barrier.*

Proof. Condition (2.9) implies that the B_{n-1}^{+*}-tail of $\phi_n^{b-k+1}(\beta_b) \cdot \ldots \cdot \phi_n^2(\beta_{k+1})\,\phi_n(\beta_k)$ is trivial. In particular the B_{n-1}^{+*}-tail of $\phi_n^2(\beta_{k+1}^{\#})\,\phi_n(\beta_k)$ is trivial. Then, Lemma 3.4 implies that the normal form of β_k contains an $a_{p,n}$-barrier. □

Example 3.6. Let us consider the braid β whose normal form is

$$a_{2,4}\,a_{1,3}\,a_{4,5}\,a_{2,4}\,a_{2,4}\,a_{3,5}\,a_{4,5}.$$

The ϕ_5-splitting of β is $(\beta_4, \beta_3, \beta_2, \beta_1)$ with

$$\beta_4 = a_{1,4}, \quad \beta_3 = a_{1,4}, \quad \beta_2 = a_{3,4}a_{1,3}a_{1,3}a_{2,4}a_{3,4} \quad \text{and} \quad \beta_1 = 1.$$

The letter $\beta_4^{\#}$ is $a_{1,4}$, hence by Lemma 3.5 the normal form of β_3 must contain an $a_{2,5}$-barrier: this is true, since $a_{1,4}$ is an $a_{2,5}$-barrier. The letter $\beta_3^{\#}$ is $a_{1,4}$. Then, again by Lemma 3.5, the normal form of β_2 has to contain an $a_{2,5}$-barrier: this is true, since the normal form of β_2 is $a_{3,4}a_{1,3}a_{1,3}a_{2,4}a_{3,4}$, which contains the $a_{2,5}$-barrier $a_{1,3}$.

3.3. **Ladders.** We have seen above in Lemma 3.5 that every normal word w of $\underline{B}^{+*}_{n-1}$ such that the B^{+*}_{n-1}-tail of $\phi_n(a_{p,n}\,\overline{w})$ is trivial contains at least one $a_{p,n}$-barrier. We shall see now that, under the same hypotheses, w contains not only one barrier, but even a sequence of overlapping barriers. Words containing such sequences are what we shall call ladders.

Definition 3.7. For $n \geqslant 3$, we say that a normal word w is an *$a_{p,n}$-ladder of height h lent on $a_{q-1,n-1}$*, if there exists a decomposition

$$w = w_0\, x_1\, w_1 \,...\, w_{h-1}\, x_h\, w_h, \tag{3.3}$$

and a sequence $p = f(0) < f(1) < ... < f(h) = n-1$ such that

(i) for each $k \leqslant h$, the letter x_k is an $a_{f(k-1),n}$-barrier of the form $a_{..,f(k)}$,

(ii) for each $k < h$, the word w_k contains no $a_{f(k),n}$-barrier,

(iii) the last letter of w is $a_{q-1,n-1}$.

By convention, any a-word whose last letter is $a_{q-1,n-1}$ is an $a_{n-1,n}$-ladder lent on $a_{q-1,n-1}$ and its height is 0. There exist no $a_{p,n}$-barrier with $n \geqslant 3$, hence there exist only $a_{1,2}$-ladders in $\underline{B}^{+*}_3$.

The concept of a ladder is easily illustrated by representing the generators $a_{p,q}$ as a vertical line from the pth line to the qth line on an n-line stave. Then, for every $k \geqslant 0$, the letter x_k looks like a bar of a ladder—see Figure 5.

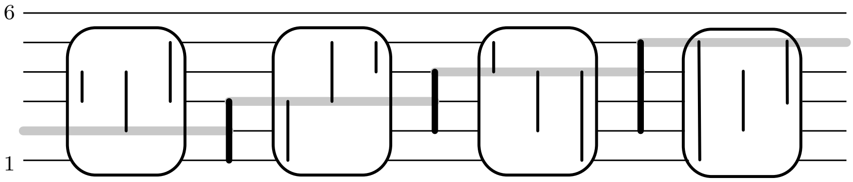

FIGURE 5. An $a_{2,5}$-ladder lent on $a_{3,5}$ (the last letter). The gray line starts at position 2 and goes up to position 5 using the bars of the ladder. The empty spaces between bars in the ladder are represented by a framed box. In such boxes the vertical line representing the letter $a_{i,j}$ does not cross the gray line. The bars of the ladder are represented by black thick vertical lines.

Our aim is to prove that the normal form of each non-terminal entry in a ϕ_n-splitting is a ladder. In order to do that, we begin with a preparatory lemma showing that barriers necessarily occur after certain letters of a normal form. Applying this result repeatedly will eventually provide us with a ladder.

Lemma 3.8. *Assume $n \geqslant 4$, that w is a suffix of a normal word of $\underline{B}^{+*}_{n-1}$, that $a_{p,q}$ belongs to B^{+*}_{n-2}, and that the B^{+*}_{n-1}-tail of $\phi_n(a_{p,q}\overline{w})$ is trivial. Then w contains an $a_{q,n}$-barrier.*

Proof. Let X be the set of all letters $a_{r,s}$ with $s > q$. Write $w = u\,v$ where v is the maximal suffix containing letters of X only. As, by hypothesis, the B^{+*}_{n-1}-tail of $\phi_n(a_{p,q}\overline{w})$ is trivial, the last letter of w exists and has the form $a_{..,n-1}$, hence v is nonempty.

As the letter $a_{p,q}$ does not lie in X, the word u is not empty. Let $x = a_{t,t'}$ be the last letter of u. By definition of u, we have $t' \leqslant q$. We suppose that v contains no $a_{q,n}$-barrier, *i.e.*, every letter $a_{r,s}$ of v satisfies $r \geqslant q$, and eventually derive a contradiction. By (1.3) and (1.4), we have

$$x a_{r,s} \equiv \begin{cases} a_{r,s} x & \text{for } r > q \text{ or } t' < q, \\ a_{t,s} x & \text{for } q = r = t', \end{cases}$$

which implies that x and v quasi-commute, *i.e.*, there exists an a-word v' satisfying $x\,v \equiv v'\,x$. Then $\phi_n(x)$ is a right-divisor of the braid represented by $\phi_n(a_{p,q} w)$. The hypothesis about $a_{p,q}$ and the relation $t' \leqslant q$ imply that $\phi_n(x)$ lies in B^{+*}_{n-1}, which contradicts the hypothesis that $\phi_n(a_{p,q}\,\overline{w})$ is trivial. □

We can now show that every normal word satisfying some mild additional condition is a ladder.

Proposition 3.9. *Assume $n \geqslant 3$, that β belongs to B^{+*}_{n-1} and that the B^{+*}_{n-1}-tail of $\phi_n(a_{p,n}\,\beta)$ is trivial for some $p \leqslant n-2$. Then the normal form of β is an $a_{p,n}$-ladder lent on $\beta^\#$.*

Proof. We put $f(1) = p$ and let w be the normal form of β. Lemma 3.5 implies that w admits a decomposition $w_0 x_1 w^{(0)}$, where w_0 is the maximal prefix of w that contains no $a_{p,n}$-barrier and $x_1 = a_{...,f(1)}$ is an $a_{p,n}$-barrier. By hypothesis, the B^{+*}_{n-1}-tail of the braid $\phi_n(a_{p,n}\,\overline{w})$ is trivial, *i.e.*, the B^{+*}_{n-1}-tail of $\phi_n(x_1\,\overline{w}^{(0)})$ is trivial. Assume $f(1) \neq n-1$. Lemma 3.8 implies that the word $w^{(0)}$ admits a decomposition $w_1\,x_2\,w^{(1)}$, where w_1 is the maximal prefix of $w^{(0)}$ that contains no $a_{f(1),n}$-barrier and x_2 is an $a_{f(1),n}$-barrier. The same argument repeats until we find a decomposition $w_0\,x_1\,w_1 ... x_h w^{(h)}$ with $f(h) = n-1$. Then, putting $w_h = w^{(h)}$, we have obtained for β a word representative that satisfies all requirements of Definition 3.7. □

Applying Proposition 3.9 to the successive entries of a ϕ_n-splitting allows one to deduce that its entries contain ladders.

Corollary 3.10. *Assume $n \geqslant 3$ and that $(\beta_b, ..., \beta_1)$ is a sequence in B^{+*}_{n-1} that is the ϕ_n-splitting of some braid of B^{+*}_n. Then, for each k in $\{b-1, ..., 2\}$, the normal form of β_k is a $\phi_n(\beta^\#_{k+1})$-ladder lent on $\beta^\#_k$.*

Proof. Condition (2.9) implies that the B^{+*}_{n-1}-tail of $\phi^2_n(\beta_{k+1})\phi_n(\beta_k)$ is trivial. In particular, the B^{+*}_{n-1}-tail of $\phi^2_n(\beta^\#_{k+1})\phi_n(\beta_k)$ is trivial. By Lemma 3.2, the letter $\beta^\#_{k+1}$ has the form $a_{...,n-1}$. Then Proposition 3.9 implies that the normal form of β_k is a $\phi_n(\beta^\#_{k+1})$-ladder lent on $\beta^\#_k$. □

By definition of a ladder, as the letter $a_{n-2,n-1}$ is not a barrier, if a word $w\,a_{n-2,n-1}$ is an $a_{p,n}$-ladder and w is nonempty, then w is an $a_{p,n}$-ladder lent on $a_{r-1,n-1}$ for some r—see Lemma 3.2(*iii*).

Another consequence of Proposition 3.9 is:

Corollary 3.11. *Assume $n \geqslant 3$ and that $(\beta_b, ..., \beta_1)$ is a sequence in B^{+*}_{n-1} that is the ϕ_n-splitting of some braid of B^{+*}_n. Then, for each c in $\{b-1, ..., 2\}$ such that β_c is either 1 or $a_{n-1,n}$, we have $\beta^\#_{c+1} = a_{n-2,n-1}$.*

Proof. Assume $\beta_c \in \{1, a_{n-2,n-1}\}$. Let $a_{p-1,n-1}$ be the last letter of β_{c+1}. Condition (2.9) implies that the B^{+*}_{n-1}-tail of $\phi^2_n(\beta_{c+1})\phi_n(\beta_c)$ is trivial. In particular the B_{n-1}^{+*}-tail of $\phi_n(a_{p,n}\,\beta_c)$ is trivial. Then, as the normal form of β_c contains no barrier, Proposition 3.9 implies $p = n-1$. Therefore we have $\beta_{c+1}^{\#} = a_{n-2,n-1}$. □

Example 3.12. Let us consider the braid of Example 3.6 again. Its ϕ_4-splitting is is $(\beta_4, ..., \beta_1)$ with $\beta_4 = a_{1,4}$, $\beta_3 = a_{1,4}$, $\beta_2 = a_{3,4}a_{1,3}a_{1,3}a_{2,4}a_{3,4}$ and $\beta_1 = 1$. The normal form of β_4 ends with $a_{1,4}$, hence the normal form of β_3 must be an $a_{2,5}$-ladder lent on $a_{1,4}$. This is true: here the ladder is $\varepsilon \cdot a_{1,4} \cdot \varepsilon$, and it has height 1, corresponding, with the notation of Definition 3.7, to $w_0 = \varepsilon$, $x_1 = a_{1,4}$ and $w_1 = \varepsilon$. Similarly, the normal form of β_3 ends with $a_{1,4}$, hence by Corollary 3.10, the normal form of β_2 must be an $a_{2,5}$-ladder lent on $a_{3,4}$. This is true again. Here the ladder has height 2, and its decomposition is $a_{3,4} \cdot a_{1,3} \cdot a_{1,3} \cdot a_{2,4} \cdot a_{3,4}$, corresponding, with the notation of Definition 3.7, to $w_0 = a_{3,4}$, $x_1 = a_{1,3}$, $w_1 = a_{1,3}$, $x_2 = a_{2,4}$ and $w_2 = a_{3,4}$. We observe that $a_{1,3}$ is an $a_{2,5}$-barrier and that $a_{2,4}$ is an $a_{3,5}$-barrier.

4. Reversing

In Section 3, we have established that almost every normal word is a ladder. We wish to use this result to establish Theorem 1, *i.e.*, to obtain (short) σ-definite representatives. The basic question is as follows. Starting with a braid word that contains letters σ_i with both positive and negative exponents, we shall try to obtain an equivalent word that is σ-positive—it is known that one cannot obtain both a σ-positive and a σ-negative representative, so our attempt must fail in some cases. The problem is to get rid of the letters σ_i^{-1} with maximal index i. We shall see that, without loss of generality, we can assume that the initial word consists of an initial fragment—that will be called dangerous—containing the negative letters (those with a negative exponent), followed by a normal word, hence by a ladder according to Proposition 3.9. Then, the main technical step consists in proving that the product of a dangerous word with a ladder can be transformed using a simple algorithmic process called reversing into an equivalent σ-positive word: roughly speaking, ladders protect against dangerous elements.

4.1. D-words.

Up to now, we have considered braid words involving letters of two different alphabets, namely the Artin generators σ_i and the Birman–Ko–Lee generators $a_{p,q}$. From now on, we shall also use a third alphabet, corresponding to the following braids.

Definition 4.1. For $1 \leqslant p < q$, we put

$$d_{p,q} = a_{p,p+1}\, a_{p+1,p+2} \cdots a_{q-1,q} \;(\,= \sigma_p\sigma_{p+1} \cdots \sigma_{q-1}).$$

So, in particular, the equalities

$$a_{p,q} = d_{p,q}d_{p,q-1}^{-1} = d_{p,q-1}\;\sigma_{q-1}\;d_{p,q-1}^{-1} \tag{4.1}$$

hold for $1 \leqslant p < q$.

Hereafter it is convenient to use $d_{p,q}$ as a single letter. In this context, a word on the letters $d_{p,q}^{\pm1}$ (*resp.* $a_{p,q}^{\pm1}$ and $d_{p,q}^{\pm1}$, *resp.* $\sigma_i^{\pm1}$) will be called a *d-word* (*resp.* an *ad-word*, *resp.* a σ-word). We adopt the convention that the d-word $d_{p,p}$ is the empty word ε for all p.

All words over the above alphabets represent braids, and they can be translated into σ-words. It is coherent with the intended braid interpretations to define words $\underline{a}_{p,q}$ and $\underline{d}_{p,q}$ by

$$\underline{a}_{p,q} = \sigma_p ... \sigma_{q-2}\sigma_{q-1}\sigma_{q-2}^{-1}...\sigma_p^{-1}, \quad \underline{d}_{p,q} = \sigma_p...\sigma_{q-1}. \tag{4.2}$$

In this way, for each ad-word w, the braid represented by w coincides with the braid represented by the σ-word $\underline{w}$ obtained from w by replacing every letter $a_{p,q}$ by $\underline{a}_{p,q}$ and every letter $d_{p,q}$ by $\underline{d}_{p,q}$, and no ambiguity can result from using different alphabets. Of course, if w and w' are two ad-words, we declare that $w \equiv w'$ is true if the σ-words $\underline{w}$ and $\underline{w}'$ are equivalent under the braid relations (1.1). Note in particular that the braid represented by the d-word $d_{1,n}$ is the Garside braid δ_n.

The following equivalences of ad-words easily result from the definitions.

Lemma 4.2. *The following relations are satisfied:*

$$\begin{aligned} d_{p,r} &\equiv d_{p,q}\ d_{q,r} && \textit{for } p < q < r, && \text{(4.2.i)}\\ \phi_n(d_{p,q}) &\equiv d_{p+1,q+1} && \textit{for } p < q \leqslant n-1, && \text{(4.2.ii)}\\ d_{p,q}\ d_{r,s} &\equiv d_{r,s}\ d_{p,q} && \textit{for } p < q < r < s, && \text{(4.2.iii)}\\ d_{r,s}^{-1}\ a_{p,q}\ d_{r,s} &\equiv \phi_s^{-1}\big(\phi_r(a_{p,q})\big) && \textit{for } p < q \leqslant r < s. && \text{(4.2.iv)} \end{aligned}$$

Proof. Relation (4.2.i) holds by definition of $d_{p,q}$. Relation (4.2.ii) is an immediate consequence of (1.7). For (4.2.iii), we observe that the σ_i of greatest index occurring in $d_{p,q}$ is σ_{q-1}, while the σ_i of lower index occurring in $d_{r,s}$ is σ_r. As $q < r$ implies $q-1 \leqslant r-2$, we can apply the Artin commutativity relation of (1.1) to obtain the expected result.

It remains to prove (4.2.iv). First, (4.2.i) implies $d_{1,s} \equiv d_{1,r}\, d_{r,s}$, hence $d_{r,s} \equiv d_{1,r}^{-1}\, d_{1,s}$. We deduce $d_{r,s}^{-1}\ a_{p,q}\ d_{r,s} \equiv d_{1,s}^{-1}\ d_{1,r}\, a_{p,q}\, d_{1,r}^{-1}\ d_{1,s}$. As, by hypothesis, $a_{p,q}$ lies in B_r^{+*}, the subword $d_{1,r}\, a_{p,q}\, d_{1,r}^{-1}$ is equivalent to $\phi_r(a_{p,q})$. Finally the conjunction of $B_r^{+*} \subseteq B_s^{+*}$ and $\phi_r(a_{p,q}) \in B_r^{+*}$ implies $d_{1,s}^{-1}\, \phi_r(a_{p,q})\, d_{1,s} \equiv \phi_s^{-1}\big(\phi_r(a_{p,q})\big)$. □

4.2. Sigma-positive words.

Our aim is to obtain σ-positive and σ-negative representative words. We shall need slightly more precise versions of these notions.

Definition 4.3. (i) A σ-word w is called σ_i*-positive* (resp. σ_i-negative) if w contains at least one letter σ_i, no letter σ_i^{-1} (resp. at least one letter σ_i^{-1} and no letter σ_i) and no letter $\sigma_j^{\pm 1}$ for $j \geqslant i$.

(ii) A σ-word w is said to be σ_i*-nonnegative* if it is σ_i-positive, or it does not contain the letter $\sigma_j^{\pm1}$ with $j \geqslant i$.

(iii) An ad-word w is called σ_i-positive (resp. σ_i-negative, resp. σ_i-nonnegative) if the word $\underline{w}$ is σ_i-positive (resp. σ_i-negative, resp. σ_i-nonnegative).

Example 4.4. A σ-word cannot be simultaneously σ_i-positive and σ_i-negative, but, on the other hand, a σ-word can be neither σ_i-positive nor σ_i-negative for any i. For instance, $\sigma_2\sigma_1\sigma_2^{-1}$ is neither σ_2-positive (since it contains a letter σ_2^{-1}), nor σ_2-negative (since it contains a letter σ_2), nor σ_1-positive or σ_1-negative (since it contains a letter σ_2). By contrast, the equivalent word $\sigma_1^{-1}\sigma_2\sigma_1$ is σ_2-positive. On the other hand, the empty word, σ_1^{-1}, and $\sigma_2\,\sigma_1^{-1}$ are σ_2-nonnegative words, since the letter σ_2^{-1} does not occur in it.

As for a-words, $a_{2,3}^{-1}a_{1,3}$ is not σ_2-positive, since its translation under (4.2) is the σ-word $\sigma_2^{-1}\sigma_1\sigma_2\sigma_1^{-1}$, which is not σ_2-positive as it contains the letter σ_2^{-1}. However, the previous a-word is equivalent to the a-word $a_{1,3}a_{1,2}^{-1}$, which translates into $\sigma_1\sigma_2\sigma_1^{-1}\sigma_1^{-1}$ and is therefore σ_2-positive, since $\sigma_1\sigma_2\sigma_1^{-1}\sigma_1^{-1}$ contains one letter σ_2 and no letter σ_2^{-1}.

An immediate consequence of Definition 4.3(*iii*) is

Lemma 4.5. *An ad-word w is σ_i-positive if w contains at least one letter $a_{..,i+1}$ or $d_{..,i+1}$, and no letter $a^{-1}_{..,i+1}$, $d^{-1}_{..,i+1}$, $a^{\pm1}_{..,j}$, or $d^{\pm1}_{..,j}$ with $j > i+1$.*

4.3. **Dangerous words.** We arrive at a key notion. The problem is to identify the generic form of the σ-negative fragments we wish to control and, possibly, get rid of. It turns out that the convenient notion is defined in terms of the letters $d^{-1}_{p,q}$, and it is what we call a dangerous word.

Definition 4.6. For $n \geqslant 3$, a d-word is called *$a_{p,n}$-dangerous of type q* if it has the form

$$d^{-1}_{f(d),n-1}\, d^{-1}_{f(d-1),n-1} \,...\, d^{-1}_{f(1),n-1} \tag{4.4}$$

with $q = f(d) \geqslant f(d-1) \geqslant ... \geqslant f(1) = p$.

By convention the unique $a_{n-1,n}$-dangerous word is the empty word.

Note that a dangerous d-word w is completely determined by the σ-word $\underline{w}$. Indeed, we recover w from $\underline{w}$ by gathering the σ_i^{-1}'s and cutting before each letter σ^{-1}_{n-2}. For instance, $\sigma_3^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}$ can only be the translation of the $a_{1,5}$-dangerous word $d^{-1}_{2,4}d^{-1}_{1,4}$.

At this point, the definition of a dangerous word comes out of a hat. For the moment, let us observe that the letter $a_{p,n}$ is equivalent to $d_{p,n}d^{-1}_{p,n-1}$. In this expression, $d^{-1}_{p,n-1}$, which is $a_{p,n}$-dangerous, corresponds to the negative fragment of $a_{p,n}$. This reflects the intuition that dangerous words are associated with the negative parts of a-words—hence with their dangerous parts in view of our aim, which is to find σ-positive expressions.

4.4. **The reversing algorithm.** The aim of this section is to describe an algorithm that, starting with an $a_{p,n}$-dangerous word u and an $a_{p,n}$-ladder w, returns a σ_{n-2}-positive word w' that is equivalent to $u\,w$ and that is close to be an $a_{p,n}$-ladder in a sense that will be defined below.

The basic ingredient is a process called *reversing* that transforms (certain) ad-words with letters $d^{-1}_{..,n-1}$ on the left into equivalent words with letters $d^{-1}_{..,n-1}$ on the right (or with no letter $d^{-1}_{..,n-1}$ at all). Thus reversing is a process for pushing letters $d^{-1}_{..,n-1}$ to the right.

Definition 4.7. Let w, w' be ad-words. We declare that $w \curvearrowright^{(1)} w'$ is true if w' is obtained from w by replacing a subword u of w by a word u' such that (u, u') is one of the pairs

$$(d^{-1}_{p,n-1}a_{r,s},\quad R_p(a_{r,s})\, d^{-1}_{p,n-1}) \qquad \text{with } s \leqslant p \leqslant n-2 \text{ or } p \leqslant r \leqslant n-2, \tag{4.5}$$

$$(d^{-1}_{p,n-1}a_{r,s},\quad d_{r,n-1}R'_p(a_{r,s})\, d^{-1}_{s,n-1}) \qquad \text{with } r < p < s \leqslant n-1, \tag{4.6}$$

$$(d^{-1}_{p,n-1}d_{r,n-1},\quad d_{r,n-1}\, R''_p) \qquad \text{with } r < p \leqslant n-2, \tag{4.7}$$

with

$$R_p(a_{r,s}) = \begin{cases} a_{r,n-1} & \text{for } s = p, \\ a_{r,s} & \text{for } s < p, \\ a_{s-1,n-1} & \text{for } r = p, \\ a_{r-1,s-1} & \text{for } r > p. \end{cases}, \qquad \begin{array}{l} R'_p(a_{r,s}) = d^{-1}_{p-1,n-2}\, d^{-1}_{r,s-1}, \\ \\ R''_p = d^{-1}_{p-1,n-2}. \end{array}$$

We say that w *reverses* to w', denoted $w \curvearrowright w'$, if there exists a sequence of words $w_0,w_1,...,w_\ell$ satisfying $w_0 = w$, $w_\ell = w'$, and $w_k \curvearrowright^{(1)} w_{k+1}$ for every k.

Before giving an example, we introduce the notion of a reversing diagram, which enables one to conveniently illustrate the reversing process. Assume that $w_0, w_1, \dots, w_\ell$ is a reversing sequence, *i.e.*, is a sequence of ad-words such that $w_k \curvearrowright^{(1)} w_{k+1}$ holds for every k. First, we associate with w_0 a path labeled with the successive letters of w_0: we associate to every letter $d_{p,n-1}^{-1}$ a vertical down-oriented edge labeled $d_{p,n-1}$, and to every other letter x a horizontal right-oriented edge labeled x. Then, we successively represent the words $w_1, \dots, w_\ell$ as follows : if w_{k+1} is obtained from w_k by replacing $d_{p,n-1}^{-1}\,x$ by $u\,d_{q,n-1}^{-1}$ (where $d_{p,n-1}^{-1}\,x \curvearrowright u\,d_{q,n-1}^{-1}$ holds), then we complete the pattern associated with the subword $d_{p,n-1}^{-1}\,x$ using right-oriented edges labeled u and down-oriented edge labeled $d_{q,n-1}$, see Figure 6.

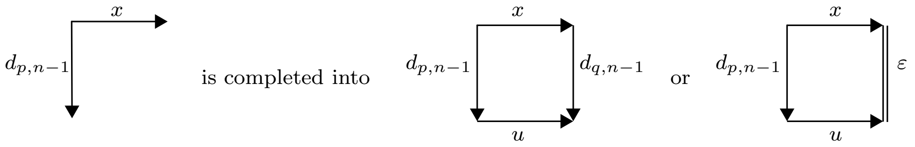

FIGURE 6. Reversing of $d_{p,n-1}^{-1}\,x$ into $u\,d_{q,n-1}$. We replace the down-oriented edge labeled $d_{q,n-1}$ by a vertical double line labeled ε whenever the relation $q = n-1$ holds, *i.e.*, $d_{q,n-1} \equiv \varepsilon$ holds.

Assume that w and w' are ad-words and w reverses to w'. Then the reversing sequence going from w to w' is not unique in general, but the resulting reversing diagram depends on w and w' only. Reversing can easily be turned into a (deterministic) algorithm by choosing to always reverse the rightmost possible subword. The algorithm terminates when a word with no subword $d_{p,n-1}^{-1}\,x$ satisfying $d_{p,n-1}^{-1}\,x \curvearrowright u'$ for some u' has been obtained. This algorithm is called *reversing algorithm.* See Figure 7 for an example.

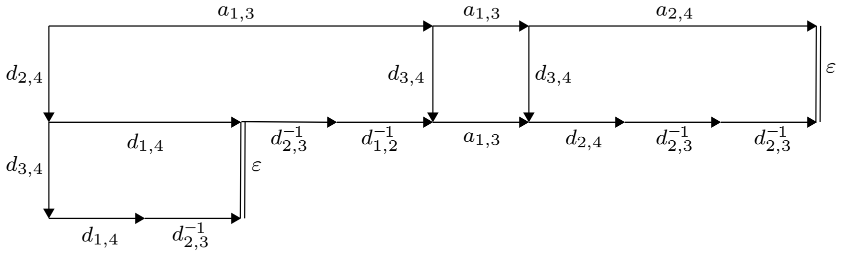

FIGURE 7. Reversing diagram of $d_{3,4}^{-1}\,d_{2,4}^{-1}\,a_{1,3}\,a_{1,3}\,a_{2,4}$. We end with $d_{1,4}\,d_{2,3}^{-1}\,d_{2,3}^{-1}\,d_{1,2}^{-1}\,a_{1,3}\,d_{2,4}\,d_{2,3}^{-1}\,d_{2,3}^{-1}$. Each rectangle in the diagram corresponds to one relation $u \curvearrowright^{(1)} u'$, hence the number of rectangles is the length of every reversing sequence $(w_0, \dots, w_\ell)$ from w_0 to w_ℓ: the sequence is not unique, but its length and the corresponding diagram are.

Remark 4.8. Formally, the above notion of reversing is similar to the transformation called "word reversing" in [9]. However, similarity is superficial only: what is common is the idea of iteratively pushing some specific factors to the right, but the considered factors and the basic switching rules are completely different.

The first, easy observation is that reversing transforms a braid word into an equivalent braid word.

Lemma 4.9. *For w, w' ad-words, $w \curvearrowright w'$ implies $w \equiv w'$.*

Proof. A simple verification. It is sufficient to prove that $w \curvearrowright^{(1)} w'$ implies $w \equiv w'$, hence to prove that $u \equiv u'$ holds for each pair (u, u') of Definition 4.7. We start with (4.5). Assume first $s \leqslant p$. Relation (4.2.iv) implies

$$d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv \phi_{n-1}^{-1}(\phi_p(a_{r,s})). \tag{4.8}$$

For $s < p$, we have $\phi_p(a_{r,s}) = a_{r+1,s+1}$, and (4.8) implies $d_{p,n-1}^{-1}\, a_{r,s} \equiv a_{r,s}\, d_{p,n-1}^{-1}$. For $s = p$, we have $\phi_p(a_{r,s}) = a_{1,r+1}$, and (4.8) implies $d_{p,n-1}^{-1}\, a_{r,s} \equiv a_{r,n-1}\, d_{p,n-1}^{-1}$.

Assume now $r \geqslant p$. Relation (4.2.i) implies $d_{p,n-1} \equiv d_{1,p}^{-1}\, d_{1,n-1}$, hence

$$d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv d_{1,n-1}^{-1}\, d_{1,p}\, a_{r,s}\, d_{1,p}^{-1}\, d_{1,n-1}. \tag{4.9}$$

For $r > p$, (4.1) with (4.2.iii) imply that $d_{1,p}$ and $a_{r,s}$ commute. Then, (4.9) gives $d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv \phi_{n-1}^{-1}(a_{r,s})$, *i.e.*, $d_{p,n-1}^{-1}\, a_{r,s} \equiv a_{r-1,s-1}\, d_{p,n-1}^{-1}$. For $r = p$, Relation (4.1) gives $d_{1,p}\, a_{r,s}\, d_{1,p}^{-1} = a_{1,s}$. Then, (4.9) gives $d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv \phi_{n-1}^{-1}(a_{1,s})$, *i.e.*, $d_{p,n-1}^{-1}\, a_{r,s} \equiv a_{s-1,n-1}\, d_{p,n-1}^{-1}$.

Next, we consider (4.7). Relation (4.2.i) implies $d_{r,n-1} \equiv d_{1,r}^{-1}\, d_{1,n-1}$, hence

$$d_{r,n-1}^{-1}\, d_{p,n-1}^{-1}\, d_{r,n-1} \equiv d_{1,n-1}^{-1}\, d_{1,r}\, d_{p,n-1}\, d_{1,r}^{-1}\, d_{1,n-1}. \tag{4.10}$$

By (4.2.iii), $d_{1,r}$ and $d_{p,n-1}$ commute, hence $d_{1,r}\, d_{p,n-1}\, d_{1,r}^{-1} \equiv d_{p,n-1}$ holds. Then, (4.10) implies $d_{r,n-1}^{-1}\, d_{p,n-1}^{-1}\, d_{r,n-1} \equiv \phi_{n-1}^{-1}(d_{p,n-1}^{-1})$. From the relation (4.2.ii), we obtain $d_{p,n-1}^{-1}\, d_{r,n-1} \equiv d_{r,n-1}\, d_{p-1,n-2}^{-1}$.

Finally, we consider (4.6). By (4.1), we have $a_{r,s} \equiv d_{r,s}\, d_{r,s-1}^{-1}$. Relation (4.2.i) implies $d_{r,s} \equiv d_{r,n-1}\, d_{s,n-1}^{-1}$, hence we find

$$d_{p,n-1}^{-1}\, a_{r,s} \equiv d_{p,n-1}^{-1}\, d_{r,n-1}\, d_{s,n-1}^{-1}\, d_{r,s-1}^{-1}. \tag{4.11}$$

By (4.2.iii), the letters $d_{s,n-1}$ and $d_{r,s-1}^{-1}$ commute. Moreover, (4.7) implies that the word $d_{p,n-1}^{-1}\, d_{r,n-1}$ is equivalent to $d_{r,n-1}\, d_{p-1,n-2}^{-1}$. Hence, from (4.11), we obtain the relation $d_{p,n-1}^{-1}\, a_{r,s} \equiv d_{r,n-1}\, d_{p-1,n-2}^{-1}\, d_{r,s-1}^{-1}\, d_{s,n-1}^{-1}$. □

5. Walls

We shall now apply the reversing algorithm of Section 4.4 to those words that consist of an $a_{p,n}$-dangerous word followed by an $a_{p,n}$-ladder, with the aim of obtaining an equivalent σ_i-positive word whenever this is possible.

Once again, the problem is to identify the generic form of the final words we can obtain. A new type of braid words called *walls* occurs here, and the main result is that reversing a word consisting of a dangerous word followed by a ladder always results in a σ-nonnegative word that is a wall.

5.1. **Dangerous against ladders: case of length** 1. We first concentrate on the case when the dangerous word has length 1, *i.e.*, it consists of a single negative d-letter—the general case will be handled in Section 5.3. In view of Theorems 1 and 2, we shall not only describe the resulting word *ad*-word, but also compute both the time and space complexity of the algorithm involved in the transformation.

First we introduce now the notion of a *wall*, a weak variant of a ladder. It comes in two versions called *high* and *low*.

Definition 5.1. For $n \geqslant 3$ and $p \leqslant n-2$, we say that an *ad*-word w is a *high $a_{p,n}$-wall lent on $a_{q-1,n-1}$* if there exists a decomposition

$$w = u \cdot d_{r,n-1} \cdot w' \cdot d_{q-1,n-1} \cdot v$$

such that

– u is a positive a-word, (5.1.i)
– $r < p$ holds, (5.1.ii)
– w' is a σ_{n-2}-nonnegative *ad*-word, (5.1.iii)
– v is $a_{q-1,n-1}$-dangerous. (5.1.iv)

We say that an *ad*-word w is a *low $a_{p,n}$-wall lent on $a_{q-1,n-1}$* if there exists a decomposition

$$w = u \cdot d_{q-1,n-1} \cdot v$$

such that

– u is a positive a-word, (5.1.v)
– $q-1 < p$ holds, (5.1.vi)
– v is an $a_{q-1,n-1}$-dangerous of type $p' < p$. (5.1.vii)

In both cases, we write $F(w)$ for the word denoted u above, and $D(w)$ for the word denoted v above.

We say that an a-word w is an *$a_{p,n}$-wall* if it is either a high or a low $a_{p,n}$-wall.

Note that the condition satisfied by the letter $d_{r,n-1}$ occurring in the decomposition of a high wall is the condition satisfied by the $a_{p,n}$-barrier $a_{r,n-1}$. The same property holds for the letter $d_{q-1,n-1}$ occurring in the decomposition of a low wall.

So far we have defined $a_{p,n}$-walls for $p \leqslant n-2$ only. We now consider $a_{n-1,n}$-walls, which are special as are $a_{n-1,n}$-ladders.

Definition 5.2. For $n \geqslant 3$, we say that an *ad*-word w is an *$a_{n-1,n}$-wall lent on $a_{q-1,n-1}$* if w can be decomposed as $u \cdot d_{q-1,n-1} \cdot v$ with u a positive a-word and v an $a_{q-1,n-1}$-dangerous word. Then we define $F(w) = u$ and $D(w) = v$.

By definition, every $a_{p,n}$-wall lent on $a_{q-1,n-1}$ is also an $a_{r,n}$-wall lent on $a_{q-1,n-1}$ for $r \geqslant p$.

Walls are introduced in order to describe the output of the reversing algorithm running on those words that consist of an $a_{p,n}$-dangerous word followed by an $a_{p,n}$-ladder.

Lemma 5.3. *Let w be an $a_{p,n}$-ladder lent on $a_{q-1,n-1}$ with $p \leqslant n-2$ and $n \geqslant 3$. Let $w_0\, x_1 \,...\, x_h\, w_h$ be the decomposition of w as a ladder. Then $d_{p,n-1}^{-1}\, w$ is equivalent to an $a_{p,n}$-wall w' lent on $a_{q-1,n-1}$. The latter can be computed using at most ℓ reversing steps plus one basic operation, and it satisfies*

– $|F(w')| = |w_0|$, (5.3.i)
– $|D(w')| \leqslant 2$, (5.3.ii)
– $|w'| \leqslant |w| + 2(h-1) + 2|w_h| + |D(w')|$, (5.3.iii)
– *w' is a high wall for $w_h \neq \varepsilon$.* (5.3.iv)

Proof. The main idea is illustrated in Figure 8: starting with $d_{p,n-1}^{-1}\, w$, *i.e.*, with $d_{p,n-1}^{-1}\, w_0\, x_1 \,...\, x_h\, w_h$, we reverse the diagram by pushing the vertical (negative) d-arrows to the right until a wall is obtained. The success at each elementary step is guaranteed by Lemma 4.9. In general we obtain a high wall. A few particular

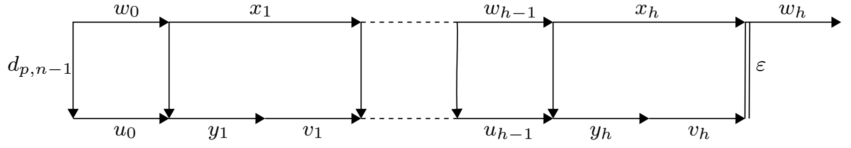

FIGURE 8. Reversing $d_{p,n-1}^{-1}\,w$ into a wall when w is a ladder (proof of Lemma 5.3).

cases have to be considered separately, namely when w_h is empty, in which case we obtain a low wall if the height h is 1.

We start with a description of elementary blocks of the diagram of Figure 8. Write $x_k = a_{e(k),f(k)}$ for $k = 1, ..., h$, and put $f(0) = p$. Fix k with $0 \leqslant k \leqslant h-1$. Put $u_k = R_{f(k)}(w_k)$, $y_{k+1} = d_{e(k+1),n-1}$ and $v_{k+1} = R'_{f(k)}(x_{k+1})$. Then, we have $d_{f(k),n-1}^{-1}\,w_k\,x_{k+1} \curvearrowright u_k\,y_{k+1}\,v_{k+1}\,d_{f(k+1),n-1}^{-1}$, corresponding to the diagram

$$\begin{tikzcd}
{} \arrow[r, "w_k"] \arrow[d, "d_{f(k),n-1}"'] & {} \arrow[rr, "x_{k+1}"] \arrow[d, "d_{f(k),n-1}"] & & {} \arrow[d, "d_{f(k+1),n-1}"] \\
{} \arrow[r, "u_k"'] & {} \arrow[r, "y_{k+1}"'] & {} \arrow[r, "v_{k+1}"'] & {}
\end{tikzcd}$$

Gathering the reversing diagrams corresponding to the successive values of the parameter k, we precisely obtain the diagram of Figure 8. Put $w'_k = u_k\,y_{k+1}\,v_{k+1}$ for $0 \leqslant k \leqslant h-1$.

At this point, we have to consider three slightly different cases. Assume first $w_h = \varepsilon$ and $h \geqslant 2$, the easiest case, of which the other two cases will be derived.

Put $w' = w'_0 ... w'_{h-1}$. By construction, we have $d_{p,n-1}^{-1}\,w \curvearrowright w'$. Hence, by Lemma 4.9, $d_{p,n-1}^{-1}\,w$ is equivalent to w'. We shall now prove that w' is a wall of the expected type, and that the complexity statements are satisfied.

As w_h is empty, the last letter of w is x_h. This implies $x_h = a_{q-1,n-1}$, hence $y_h = d_{q-1,n-1}$. Put $w'' = v_1\,w'_2 ... w'_{h-2}\,u_{h-1}$. By construction, we have

$$w' = u_0 \cdot d_{e(1),n-1} \cdot w'' \cdot d_{q-1,n-1} \cdot v_h.$$

We shall now check that w' is a high $a_{p,n}$-wall lent on $a_{q-1,n-1}$. As the image of an a-letter under R_p is an a-letter, the word u_0 is a positive a-word whose length is $|w_0|$. Hence (5.1.i) and (5.3.i) are satisfied.

Next, by definition of a ladder, the letter x_1 is an $a_{p,n}$-barrier, hence $e(1) < p$ holds, *i.e.*, (5.1.ii) is satisfied.

As the words u_k, y_{k+1}, v_{k+1} are σ_{n-2}-nonnegative, the word w'' is also σ_{n-2}-nonnegative. So (5.1.iii) holds.

Now, we recall that v_h is equal to $d_{f(h-1)-1,n-2}^{-1}\,d_{e(h),n-2}^{-1}$ with $e(h) = q-1$. By definition of a ladder, the letter x_h is an $a_{f(h-1),n}$-barrier. Therefore, we have $q-1 < f(h-1)$, which implies $f(h-1) - 1 \geqslant q-1$. Hence v_h is $a_{q-1,n-1}$-dangerous of length 2. So (5.1.iv) and (5.3.ii) are satisfied.

Finally, for (5.3.iii), we compute

$$|w'_k| = |u_{k-1}| + |y_k| + |v_k| = |w_{k-1}| + 1 + 2 = |w_{k-1}\,x_k| + 2.$$

Then, as w_h is empty, we obtain

$$|w'| = \sum_{k=0}^{h-1} |w'_k| = \sum_{k=0}^{h-1} |w_k\, x_{k+1}| + 2h = |w| + 2h.$$

As in this case w_h is empty and the length of $D(w')$ is 2, *i.e.*, the length of v_h is 2, Condition (5.3.iii) holds. So the case of w_h empty with $h \geqslant 2$ is completed, except for the time complexity analysis.

Assume now $w_h = \varepsilon$ and $h = 1$. Then w' is equal to $u_0 \cdot d_{q-1,n-1} \cdot v_1$. As in the previous case, the word u_0 is a positive a-word of length w_0 and we have $|w'| = |w|+2$. The word v_1 is equal to $d^{-1}_{p-1,n-2}\, d^{-1}_{q-1,n-2}$, which is $a_{q-1,n-1}$-dangerous of type $p-1$ and has length 2. Therefore, w' is a low $a_{p,n}$-wall lent on $a_{q-1,n-1}$ satisfying (5.3.i), (5.3.ii) and (5.3.iii).

Assume finally $w_h \neq \varepsilon$. Then, we decompose w_h as $w''_h\, a_{q-1,n-1}$. Put

$$w' = w'_0 \,...\, w'_{h-1}\, w''_h\, d_{q-1,n-1}\, d^{-1}_{q-1,n-2},$$

and $w'' = v_1\, w'_2 \,...\, w'_{h-1}\, w''_h$. We have $w' = u_0 \cdot d_{f(1),n-1} \cdot w'' \cdot d_{q-1,n-1} \cdot d^{-1}_{q-1,n-2}$. Then (5.1.i), (5.1.ii), (5.1.iii) are checked as in the case $w_h = \varepsilon$. By construction, the word $d^{-1}_{q-1,n-2}$ is $a_{q-1,n-1}$-dangerous of length 1. So (5.1.iv) and (5.3.ii) are satisfied. Then, by definition of w', (5.3.iv) holds. We check now (5.3.iii). Starting form $|w'_k| = |w_{k-1}\, x_k| + 2$, we obtain

$$|w'| = \sum_{k=0}^{h-1} |w'_k| + |w''_h| + 2 = \sum_{k=0}^{h-1} |w_k\, x_{k+1}| + |w_h| + 2h + 1 = |w| + 2h + 1.$$

As w_h is not empty, we have $|w_h| \geqslant 1$, hence $2|w_h| \geqslant 2$. Moreover, in this case, the length of $D(w')$ is 1. Therefore, we get $3 \leqslant 2|w_h| + |D(w')|$, and eventually find

$$|w'| \leqslant |w| + 2(h-1) + 2|w_h| + |D(w')|.$$

So, all cases have been considered. It only remains to consider the time complexity. In the first and second cases, at most $|w|$ reversing operations are needed. In the last case—$w_h \neq \varepsilon$—at most $|w|$ reversing operations are needed, plus the decomposition of $w^{\#}_h$ into two d-letters. □

Example 5.4. We saw in Example 3.12 that the word $w = a_{3,4}\, a_{1,3}\, a_{1,3}\, a_{2,4}\, a_{3,4}$ is an $a_{2,5}$-ladder lent on $a_{3,4}$. Let us compute the $a_{2,5}$-wall lent on $a_{3,4}$ that is equivalent to $d^{-1}_{2,5}\, w$. Applying the reversing algorithm to $d^{-1}_{2,4}\, w$ gives

$$w'' = a_{2,3}\, d_{1,4}\, d^{-1}_{1,3}\, d^{-1}_{1,2}\, a_{1,4}\, d_{2,4}\, d^{-1}_{2,3}\, d^{-1}_{2,3}\, a_{3,4} \quad \text{(see Figure 9).}$$

The word w'' is not a wall because its last letter does not have the correct form. However, if we replace the last letter $a_{3,4}$ of w'' by $d_{3,4}$ we obtain the high wall

$$w' = a_{2,3} \cdot d_{1,4} \cdot d^{-1}_{1,3}\, d^{-1}_{1,2}\, a_{1,4}\, d_{2,4}\, d^{-1}_{2,3}\, d^{-1}_{2,3} \cdot d_{3,4} \cdot \varepsilon.$$

The word $F(w')$ of w' is $a_{2,3}$, whereas $D(w')$ is empty.

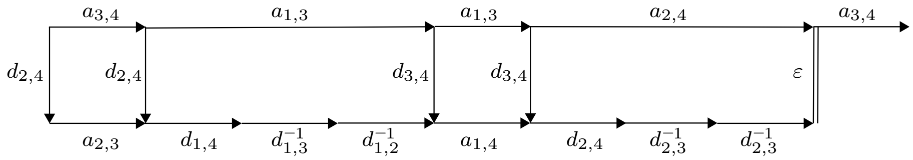

FIGURE 9. Reversing diagram of the word $d^{-1}_{2,4}\, a_{3,4}\, a_{1,3}\, a_{1,3}\, a_{2,4}\, a_{3,4}$.

5.2. **Dangerous against wall.** In the previous section, we studied the action of the reversing algorithm running on a word $u\,w$ in the special case when u is an $a_{p,n}$-dangerous word of length 1 and w is an $a_{p,n}$-ladder. We proved that the output word is an $a_{p,n}$-wall. Before turning to the general case of an initial dangerous word with an arbitrary length—that will be done in the next section—we consider here the case of an $a_{p,n}$-dangerous word of length 1 followed by an $a_{p,n}$-wall. The result is that the output word is again an $a_{p,n}$-wall. This shows that, contrary to the family of ladders, the family of walls enjoys good closure properties that will make inductive arguments possible.

We start with a technical result that will be used twice in the proof of Lemma 5.6.

Lemma 5.5. *Assume $n \geqslant 3$, that w is a positive a-word containing an $a_{p,n}$-barrier and that $r < p$ holds. Then the word $d^{-1}_{p,n-1}\, w\, d_{r,n-1}$ reverses to the ad-word*

$$u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d^{-1}_{s-1,n-2},$$

which is obtained in at most $|w| + 1$ steps and satisfies

– $t < p$ *and* $r < s$, (5.5.i)
– u *is a positive a-word with* $|u| < |w|$, (5.5.ii)
– u' *is a* σ_{n-2}*-nonnegative ad-word,* (5.5.iii)
– $|u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d^{-1}_{s-1,n-2}| \leqslant |w\, d_{r,n-1}| + 2|w| - 2|u| + 1.$ (5.5.iv)

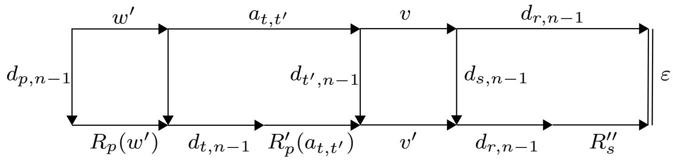

FIGURE 10. Reversing $d^{-1}_{p,n-1}\, w$ into a wall in the case when w is a wall (proof of Lemma 5.5).

Proof. Write w as $w'\, a_{t,t'}\, v$ where w' is the maximal prefix of w that contains no $a_{p,n}$-barrier, and with $a_{t,t'}$ an $a_{p,n}$-barrier. The argument is illustrated in Figure 10: starting with $d^{-1}_{p,n-1}\, w\, d_{r,n-1}$, we reverse the diagram by pushing the vertical (negative) d-arrows to the right until a wall is obtained. The success at each elementary step is guaranteed by Lemma 4.9.

As w' does not contains any $a_{p,n}$-barrier, we have $d^{-1}_{p,n-1}\, w' \curvearrowright R_p(w')\, d^{-1}_{p,n-1}$. By construction $a_{t,t'}$ is an $a_{p,n}$-barrier, *i.e.*, $t < p < t'$ holds. We deduce

$$d^{-1}_{p,n-1}\, a_{t,t'} \curvearrowright d_{t,n-1} R'_p(a_{t,t'})\, d^{-1}_{t',n-1}.$$

By definition of elementary reversing steps, we obtain $d^{-1}_{t',n-1}\, v \curvearrowright v'\, d^{-1}_{s,n-1}$ for some ad-word v' with $|v'| \leqslant 3|v|$ and some $s \geqslant t'$. The hypothesis $r < p$ together with $p < t'$ and $t' \leqslant s$ implies $r < s$. Hence $d^{-1}_{s,n-1}\, d_{r,n-1} \curvearrowright d_{r,n-1}\, R''_s$ holds.

Write $u = R_p(w')$ and $u' = R'_p(a_{t,t'})\, v'$. By construction, we have

$$d^{-1}_{p,n-1}\, w\, d_{r,n} \curvearrowright u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d^{-1}_{s-1,n-1},$$

and we claim that the latter word has the expected properties.

Condition (5.5.i) is an immediate consequence of the above results.

As the image of an a-letter under R_p is an a-letter, the word u is a positive a-word of length $|w'|$. By definition, the word w' is a proper prefix of w. Then $|w'| < |w|$ holds, *i.e.*, (5.5.ii) is satisfied.

By definition of elementary reversing steps, the image of a positive a-word under R and R' is σ_{n-2}-nonnegative, hence the word v' is σ_{n-2}-nonnegative. As $R'_p(a_{t,t'})$ is σ_{n-2}-nonnegative, the word u' is σ_{n-2}-nonnegative, *i.e.*, (5.5.iii) holds.

For (5.5.iv), we compute

$$|u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d^{-1}_{s-1,n-2}| = |w'| + |u'| + 3 = |w'| + |v'| + 5.$$

By construction of v', we have $|v'| \leqslant 3|v|$. Using $|w| = |w'| + 1 + |v|$, we deduce

$$\begin{aligned}|u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d^{-1}_{s-1,n-2}| &\leqslant 3|w| - 2|w'| + 2\\ &= |w\, d_{p,n-1}| + 2(|w| - |w'|) + 1,\end{aligned}$$

which is the expected inequality since $|w'|$ is equal to $|u|$ by (5.5.ii).

An easy bookkeeping argument gives the bound on the number of steps in the revering process. □

We are now able to establish the main result of this section.

Lemma 5.6. *Assume that w is an $a_{p,n}$-wall lent on $a_{q-1,n-1}$. Then $d^{-1}_{p,n-1}w$ reverses in at most $|F(w)| + 1$ steps to an $a_{p,n}$-wall w' satisfying*

– $|F(w')| \leqslant |F(w)|$, (5.6.i)
– $|D(w')| \leqslant |D(w)| + 1$, (5.6.ii)
– $|w'| \leqslant |w| + 2|F(w)| - 2|F(w')| + 1$, (5.6.iii)
– *w' is a high wall whenever w is a high wall.* (5.6.iv)

Proof. Assume that w is a low wall. Then w admits the decomposition $w = F(w)\, d_{q-1,n-1}\, D(w)$. By definition of a wall, we have $q - 1 < p$. First, assume in addition that $F(w)$ contains no $a_{p,n}$-barrier. Then, the reversing process gives

$$d^{-1}_{p,n-1}\, w \curvearrowright R_p(F(w))\, d^{-1}_{p,n-1}\, d_{q-1,n-1}\, D(w) \curvearrowright R_p(F(w))\, d_{q-1,n-1}\, d^{-1}_{p-1,n-2}\, D(w).$$

Write $w' = u \cdot d_{q-1,n-1} \cdot v$ with $u = R_p(F(w))$ and $v = d^{-1}_{p-1,n-2}\, D(w)$. As the image of a positive a-letter under R is a positive a-letter, the word u is a positive a-word of length $|F(w)|$. Then, $q - 1 < p$ implies that w' is a low $a_{p,n}$-wall lent on $a_{q-1,n-1}$ satisfying (5.6.i) and (5.6.ii) hold—$D(w') = v$. Condition (5.6.iii) is a direct consequence of the construction of w' together with $|v| = |D(w)| + 1$.

Next, assume in addition that $F(w)$ contains an $a_{p,n}$-barrier. By Lemma 5.5 applied to $F(w)\, d_{q-1,n-1}$, there exist two words u and u', and two integers s and t satisfying

$$d^{-1}_{p,n-1}\, w \curvearrowright u\, d_{t,n-1}\, u'\, d_{q-1,n-1}\, d^{-1}_{s-1,n-2}\, D(w).$$

Write $w' = u \cdot d_{t,n-1} \cdot u' \cdot d_{q-1,n-1} \cdot v$, with $v = d^{-1}_{s-1,n-2}\, D(w)$. Condition (5.5.i) implies that v is an $a_{q-1,n-1}$-dangerous word of length at most $|D(w)| + 1$, and that

$t < p$ holds. Then, (5.5.ii) and (5.5.iii) imply that w is a high $a_{p,n}$-wall lent on $a_{q-1,n-1}$ and it satisfies (5.6.i) and (5.6.ii). Using (5.5.iv), we compute

$$|w'| = |F(w)\, d_{q-1,n-1}| + 2|F(w)| - 2|u| + |v|,$$

which implies (5.6.iii) since we have $F(w') = u$ and $D(w') = d_{s-1,n-2}^{-1}\, D(w) = v$.

Assume now that w is a high wall. Then w admits the decomposition

$$w = F(w)\, d_{r,n-1}\, w''\, d_{q-1,n-1}\, D(w),$$

with $r < p$. First, assume that $F(w)$ contain no $a_{p,n}$-barrier. Then, reversing process gives

$$d_{p,n-1}\, w \curvearrowright R_p(F(w))\, d_{r,n-1}\, d_{p-1,n-2}^{-1}\, w''\, d_{q-1,n-1}\, D(w).$$

Write $w' = R_p(F(w)) \cdot d_{r,n-1} \cdot d_{p-1,n-2}^{-1}\, w'' \cdot d_{q-1,n-1} \cdot D(w)$. A direct verification, based on the fact that w is an high $a_{p,n}$-wall lent on $a_{q-1,n-1}$, gives that w' is an high $a_{p,n}$-wall lent on $a_{q-1,n-1}$ satisfying (5.6.i), (5.6.ii) and (5.6.iv). For (5.6.iii), we compute $|w'| = |w| + 1$.

Assume now that $F(w)$ contains an $a_{p,n}$-barrier. Then, by Lemma 5.5 applied to $F(w)\, d_{r,n-1}$, there exists two words u, u' and two integers s, t satisfying

$$d_{p,n-1}\, w \curvearrowright u\, d_{t,n-1}\, u'\, d_{r-1,n-1}\, d_{s-1,n-2}^{-1}\, w''\, d_{q-1,n-1}\, D(w).$$

Write $w' = u \cdot d_{t,n-1} \cdot u'\, d_{r-1,n-1}\, d_{s-1,n-2}^{-1}\, w'' \cdot d_{q-1,n-1} \cdot D(w)$. Condition (5.5.iii) implies that the word $u'\, d_{r-1,n-1}\, d_{s-1,n-2}^{-1}\, w''$ is σ_{n-2}-nonnegative, and even σ_{n-2}-positive. Hence, a direct verification, based on the fact that w is an high $a_{p,n}$-wall lent on $a_{q-1,n-1}$, shows that w' is a high $a_{p,n}$-wall lent on $a_{q-1,n-1}$ and it satisfies (5.6.i), (5.6.ii) and (5.6.iv). Using (5.5.iv), we compute

$$|w'| \leqslant |F(w)\, d_{r,n-1}| + 2|F(w)| - 2|u| + 1 + |w''| + 1 + |D(w)|,$$

which implies (5.6.iii) since $F(w') = u$.

As for the number of reversing steps, it follows from an easy bookkeeping argument using Lemma 5.5. □

5.3. **Dangerous against ladders: the general case.** In the previous section, we studied the action of the reversing algorithm running on a word $u\,w$ in the special case when u is $a_{p,n}$-dangerous of length 1 and w is an $a_{p,n}$-ladder. We proved that the output word is an $a_{p,n}$-wall. The aim of this section is to describe the reversing algorithm in the general case, *i.e.*, for a dangerous word of arbitrary length.

Proposition 5.7. *Assume that w is an $a_{p,n}$-ladder lent on $a_{q-1,n-1}$ and u be an $a_{p,n}$-dangerous word, with $n \geqslant 3$. Then $u\,w$ is equivalent to an $a_{p,n}$-wall w' lent on $a_{q-1,n-1}$. It can be computed using at most $|u|\,|w|$ reversing steps, plus one basic operation, hence in time $O(|u||w| + 1)$, and it satisfies*

– $|D(w')| \leqslant |u| + 1,$ (5.7.i)

– $|w'| \leqslant 3|w| + |u| - 1.$ (5.7.ii)

Moreover, if w is an $a_{p,n}$-ladder lent on $a_{n-2,n-1}$ but different from $a_{n-2,n-1}$, then w' admits the decomposition $w' = w''\, d_{n-2,n-1}$, where w'' is a σ_{n-2}-positive word.

Proof. All ladders and walls in this proof are supposed to be lent on $a_{q-1,n-1}$. We shall construct an $a_{p,n}$-wall w' that is equivalent to $u\,w$ by induction on the length of u.

Assume first $p \leqslant n-2$. Then u is not empty. Write u as $d^{-1}_{f(d),n-1} \cdot \ldots \cdot d^{-1}_{f(1),n-1}$. Define $w_{(1)}$ to be the $a_{f(1),n}$-wall of Lemma 5.3 that is equivalent to $d^{-1}_{f(1),n-1}\, w$. Starting from $w_{(1)}$, we inductively define $w_{(k+1)}$ to be the ad-word obtained by reversing $d^{-1}_{f(k+1),n-1}\, w_{(k)}$.

We claim that $w_{(k)}$ is an $a_{f(k),n}$-wall. Indeed, by definition of a wall, the relation $f(k) \geqslant f(k-1)$ implies that $w_{(k-1)}$ is also an $a_{f(k),n}$-wall. Then Lemma 5.6 guarantees that $w_{(k)}$ is an $a_{f(k),n}$-wall.

By construction, we have $u\, w \equiv w_{(d)}$. We shall now prove that $w_{(d)}$ satisfies the complexity statements.

Lemma 5.3 gives $|D(w_{(1)})| \leqslant 2$. For $1 \leqslant k \leqslant d-1$, (5.6.ii) implies $|D(w_{(k+1)})| \leqslant |D(w_{(k)})| + 1$. Hence, $|D(w_{(d)})| \leqslant |u| + 1$ holds, *i.e.*, (5.7.i) is satisfied.

Let $w_0\, x_1 \ldots x_h\, w_h$ be the decomposition of the $a_{p,n}$-ladder w. Then, by (5.6.iii), we have for each $k \geqslant 1$

$$|w_{(k+1)}| \leqslant |w_{(k)}| + 2|F(w_{(k)})| - 2|F(w_{(k+1)})| + 1. \tag{5.7}$$

Gathering the various relations (5.7) for $k = 1, \ldots, d-1$, we obtain

$$\begin{aligned} |w_{(d)}| = |w_{(d)}| &\leqslant |w_{(1)}| + 2|F(w_{(1)})| - 2|F(w_{(d)})| + d - 1 \\ &\leqslant |w_{(1)}| + 2|F(w_{(1)})| + d - 1 \end{aligned}$$

By (5.3.i), we have $|F(w_{(1)})| = |w_0|$, hence

$$|w_{(d)}| \leqslant |w_{(1)}| + 2|w_0| + d - 1.$$

Condition (5.3.iii) implies $|w_{(1)}| \leqslant |w| + 2(h-1) + 2|w_h| + |D(w_{(1)})|$. Using the relation $|w| \leqslant |w_0| + h + |w_h|$, we obtain

$$|w_{(d)}| \leqslant 3|w| + d + |D(w_{(1)})| - 3.$$

By construction, d is the length of u. As (5.3.ii) implies $|D(w_{(1)})| \leqslant 2$, we find

$$|w_{(d)}| \leqslant 3|w| + |u| - 1,$$

which completes the case $p \leqslant n-2$ writing $w' = w_{(d)}$.

Assume now $p = n-1$. Then the word u is empty. Put $w = w''\, a_{q-1,n-1}$, and write $w' = w''\, d_{q-1,n-1}\, d^{-1}_{q-1,n-2}$. The word w' is clearly an $a_{n-1,n}$-wall lent on $a_{q-1,n-1}$ and all complexities statements are satisfied. Moreover, for $q = n-1$ and $w \neq a_{n-2,n-1}$, Lemma 3.2(*iii*) implies that w'' ends with $a_{t,n-1}$ for some t, hence it is σ_{n-2}-positive. Then w' has the expected properties.

Finally, assume $p \neq n-1$, $q = n-1$ and $w \neq a_{n-2,n-1}$. Then u is not empty. By hypothesis, the last letter of w is $a_{n-2,n-1}$, which is not a barrier. Hence the word w_h is not empty and its last letter $a_{n-2,n-1}$. Then (5.3.iv) implies that the wall $w_{(1)}$ is high. Hence, (5.6.iv) implies that the wall $w_{(k)}$ is high for every $d \geqslant k \geqslant 1$, and, therefore, w' is a high wall. By definition of a high wall, w' can be expressed as $u\, d_{r,n-1}\, \widehat{w}\, d_{n-2,n-1}$. By construction, $u\, d_{r,n-1}\, \widehat{w}$ is a σ_{n-2}-positive word, so w' has all expected properties.

As for the time complexity upper bound, it follows from an easy bookkeeping argument using Lemmas 5.3 and 5.6, and the fact that the cost of one reversing step is $O(1)$. □

Example 5.8. Let w to be the $a_{3,7}$-ladder $a_{4,6}\, a_{1,4}\, a_{2,6}$ and u to be the $a_{3,7}$-dangerous word $d^{-1}_{5,6}\, d^{-1}_{3,6}\, d^{-1}_{3,6}$. The reversing diagram of $u\, w$ is displayed in Figure 11.

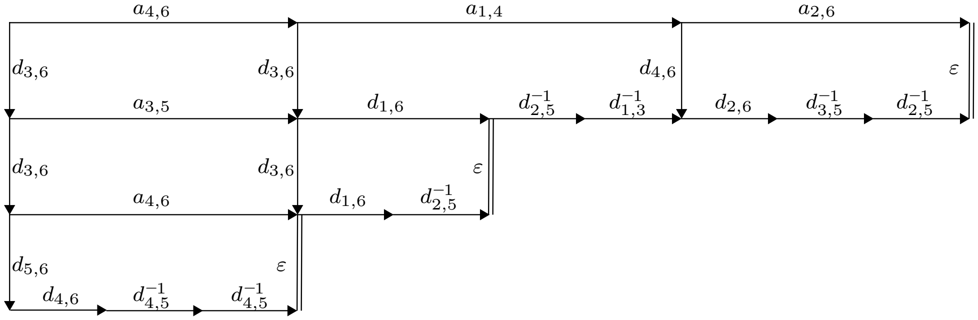

FIGURE 11. Reversing $u\,w$ into a wall. Here u is the $a_{3,7}$-dangerous word $d_{5,6}^{-1}\,d_{3,6}^{-1}\,d_{3,6}^{-1}$ and w is the $a_{3,7}$-ladder $a_{4,6}\,a_{1,4}\,a_{2,6}$, which is lent on $a_{2,6}$. With the notation of Proposition 5.7, $w_{(1)}$ is the word $a_{3,5}\,d_{1,6}\,d_{2,5}^{-1}\,d_{1,3}^{-1}\,d_{2,6}\,d_{3,5}^{-1}\,d_{2,5}^{-1}$: it can be read (from left to right) on the third row from the bottom. Then $w_{(2)}$ is the word $a_{4,6}\,d_{1,6}\,d_{2,5}^{-1}\,d_{2,5}^{-1}\,d_{1,3}^{-1}\,d_{2,6}\,d_{3,5}^{-1}\,d_{2,5}^{-1}$: it can be read on the second row, continuing on the third row when the vertical ε-labeled edge is met. Finally $w_{(3)}$ is the word $d_{4,6}\,d_{4,5}^{-1}\,d_{4,5}^{-1}\,d_{1,6}\,d_{2,5}^{-1}\,d_{2,5}^{-1}\,d_{1,3}^{-1}\,d_{2,6}\,d_{3,5}^{-1}\,d_{2,5}^{-1}$: it can be read on the bottom row, continued on the second row, and finally on the third row. The point is that we had three negative $d_{\dots,6}$-letters at first and that, at each step, we get rid of one of them, ending with a word that contains negative $d_{\dots,q}$-letters for $q \leqslant 5$ only.

We conclude the section with one more technical result, which provides the precise basic step needed in the inductive definition of our final normal form $\underline{\mathrm{NF}}_n$.

Lemma 5.9. *Assume $n \geqslant 3$, and that*
- *$(w_b, \dots, w_1)$ is the ϕ_n-splitting of a normal word w, with $b \geqslant 3$,*
- *u_b is a $w_b^{\#}$-dangerous word,*
- *c is a number in $\{b, \dots, 3\}$.*

Then, there exists
- *a σ_{n-1}-nonnegative word w',*
- *an $w_c^{\#}$-dangerous word u_c,*

both computable in time $O(|u_b||w|^2)$, that satisfy

$$d_{1,n}^{-b+3}\phi_n^{b-1}(u_b)\,\phi_n^{b-2}(w_{b-1})\dots w_1 \equiv w' \cdot d_{1,n}^{-c+3}\phi_n^{c-1}(u_c)\,\phi_n^{b-2}(w_{c-1})\dots w_1, \tag{5.8}$$

with $|w'| \leqslant 3|w_{b-1}| + \dots + 3|w_c| + |u_b| - |u_c| - b + c$ and $|u_c| \leqslant |u_b| + b$.

Proof. The idea is as follows: using induction for k going from b to $c+1$, we compute a σ_{n-1}-nonnegative word w'_{k-1} and a $w_k^{\#}$-dangerous word u_{k-1} satisfying

$$d_{1,n}^{-k+1}\,\phi_n^{k-1}(u_k)\,\phi_n^{k-2}(w_{k-1}) \equiv w'_{k-1}\,d_{1,n}^{-k+2}\,\phi_n^{k-2}(u_{k-1}). \tag{5.9}$$

Then we define w' to be $w'_{b-1}\dots w'_c$.

Let us go into details. First we construct the words w'_k and u_k. Fix k in $\{b, \dots, c+1\}$ and assume that u_k is an $w_k^{\#}$-dangerous word. Corollary 3.10 guarantees that w_{k-1} is an $\phi_n(w_k^{\#})$-ladder lent on $w_{k-1}^{\#}$. Then, by Proposition 5.7, the word $\phi_n(u_k)\,w_{k-1}$ is equivalent to a $\phi_n(w_k^{\#})$-wall v_{k-1} lent on $w_{k-1}^{\#}$. By definition of a wall, we have

$$v_{k-1} = v'_{k-1}\,d_{p-1,n-1}\,u_{k-1},$$

where v'_{k-1} is a σ_{n-2}-nonnegative word, u_{k-1} is an $w^{\#}_{k-1}$-dangerous word and $a_{p-1,n-1}$ being the last letter of w_{k-1}. Then, we obtain

$$d_{1,n}^{-k+1}\,\phi_n^{k-1}(u_k)\,\phi_n^{k-2}(w_{k-1}) \equiv d_{1,n}^{-k+1}\,\phi_n^{k-2}(v'_{k-1}\,d_{p-1,n-1}\,u_{k-1}).$$

We push the power of $d_{1,n}^{-1}$ to the last word between $d_{p-1,n-1}$ and u_{k-1}:

$$d_{1,n}^{-k+1}\,\phi_n^{k-2}(v'_{k-1}\,d_{p-1,n-1}\,u_{k-1}) \equiv \phi_n(v'_{k-1}\,d_{p-1,n-1})\,d_{1,n}^{-k+1}\,\phi_n^{k-2}(u_{k-1})$$

By Relation (4.2.i), we have $\phi_n(d_{p-1,n-1})\,d_{1,n}^{-1} \equiv d_{1,p}^{-1}$. Eventually, we obtain

$$d_{1,n}^{-k+1}\,\phi_n^{k-1}(u)\,\phi_n^{k-2}(w_{k-1}) \equiv \phi_n(v'_{k-1})\,d_{1,p}^{-1}\,d_{1,n}^{-k+2}\,\phi_n^{k-2}(u'). \tag{5.10}$$

Writing $w'_{k-1} = \phi_n(v'_{k-1})\,d_{1,p}^{-1}$, Relation (5.10) implies (5.9). By construction, w'_{k-1} is σ_{n-1}-nonnegative and u_k is an $w^{\#}_k$-dangerous word.

Gathering the relations (5.9) for k form b to $c+1$, we obtain the relation (5.8) for $w' = w'_{b-1} \dots w'_c$.

By construction, w'_k is σ_{n-1}-nonnegative for each k, hence w' is σ_{n-1}-nonnegative as well.

It remains to establish the complexity statements. For every k in $\{b, \dots, c+1\}$, (5.7.ii) implies $|v_{k-1}| \leqslant 3|w_{k-1}| + |u_k| - 1$. Then, by construction of w'_{k-1}, we have $|w'_{k-1}| \leqslant 3|w_{k-1}| + |u_k| - |u_{k-1}| - 1$. We deduce

$$|w'| = |w'_{b-1} \dots w'_c| \leqslant 3|w_{b-1} \dots w_c| + |u_b| - |u_c| - b + c.$$

For each k, (5.7.i) implies $|u_k| \leqslant |u_{k+1}|+1$. Then, we find $|u_k| \leqslant |u_b|+b-k$, hence $|u_k| \leqslant |u_b|+b$. By Proposition 5.7, computing u_k and v_k from w_k and u_{k+1} requires at most $O(|u_{k+1}||w|+1)$ steps. Therefore, computing w' and u_c from u_b and the ϕ_n-splitting of w requires at most $O((|u_b|+b)|w|+b-c)$ steps. As $b \leqslant |w|+2$ holds, we deduce that computing w' and u_c from u_b and the ϕ_n-splitting of w requires at most $O(|u_b||w|^2)$ steps. □

6. The main result

We are now ready to establish Theorems 1 and 2 of the introduction. What we shall do is to construct, for each n-strand braid β, a certain *ad*-word $\mathrm{NF}_n(\beta)$ that represents β and that is σ-definite, *i.e.*, is a word in the letters $a_{p,q}$ and $d_{p,q}$ which, translated to the alphabet of σ_i, becomes either σ-positive or σ-negative.

The construction of the word $\mathrm{NF}_n(\beta)$ involves two steps. The first (easy) step, described in Section 6.1, consists in extending the rotating normal form of Section 2.2 to all of B_n by appending convenient denominators. The process is based on the Garside structure of the monoid B_n^{+*}.

The second step starts from the rotating normal form, and it is described in Section 6.2. The process splits into three cases according to the relative position of two parameters associated with β, namely the breadth of the numerator and the exponent of the denominator in the rotating normal form of β. The reversing machinery developed in Sections 4 and 5 is needed to treat the difficult case, which is the case when the above two parameters are close one to the other.

6.1. **The rotating normal form of an arbitrary braid.** As mentioned above, we first extend the rotating normal form, so far defined only for those braids that belong to the monoid B_n^{+*}, to all braids.

Proposition 6.1. *Each braid β admits a unique expression $d_{1,n}^{-t}w$ where t is a nonnegative integer, w is a (rotating) normal word, and the braid $\overline{w}$ is not left-divisible by $d_{1,n}$ unless t is zero.*

Proof. By Proposition 1.5, the monoid B_n^{+*} is a Garside monoid with Garside element δ_n, and the group B_n is a group of fractions for the monoid B_n^{+*}. Hence, there exists a smallest integer t such that $\delta_n^t\,\beta$ belongs to the monoid B_n^{+*}. If t is positive, the minimality hypothesis implies that δ_n is not a left-divisor of $\delta_n^t\,\beta$. Taking for w the rotating normal form of $\delta_n^{-t}\,\beta$ gives a pair (t, w) of the expected form—we recall that $d_{1,n} \equiv \delta_n$ holds.

Assume that (t', w') is another pair with the above properties. Then $\delta_n^{t'}\,\beta$ belongs to B_n^{+*}, hence we have $t' \geqslant t$. If we had $t' > t$, the hypothesis $\delta_n^{-t}\,\overline{w} = \delta_n^{-t'}\overline{w'}$ would imply $\delta_n^{t'-t}\overline{w} = \overline{w'}$, implying that $\overline{w'}$ is left-divisible by δ_n, which contradicts $t' > 0$. Hence we have $t' = t$, whence $w' = w$ by uniqueness of the rotating normal form. □

Definition 6.2. The *ad*-word $d_{1,n}^{-t}w$ involved in Proposition 6.1 is called the n-rotating normal form of the braid β. The number t is called the *n-depth* of β, denoted $\mathrm{dp}_n(\beta)$; the number $t + |w|$, *i.e.*, the length of the *ad*-word $d_{1,n}^{-t}w$, is called the *n-length* of β, denoted $|\beta|_n$; finally, for $n \geqslant 3$, the n-breadth of w is called the *n-breadth* of β, denoted $\mathrm{br}_n(\beta)$.

By definition, the rotating normal form of a braid is an *ad*-word, *i.e.*, a word involving the letters $a_{p,q}$ and the letters $d_{p,q}$ (actually the letter $d_{1,n}^{-1}$ only). The terminology is coherent since, for β in B_n^{+*}, the rotating normal form as defined above coincides with the rotating normal form of Definition 2.11: indeed, β belongs to B_n^{+*} if and only if its n-depth is 0.

Building on Proposition 2.13 and on the Garside structure of B_n^{+*}, we easily see that the rotating normal form of an arbitrary braid can be computed in quadratic time.

Lemma 6.3. *For $n \geqslant 3$ and $1 \leqslant i \leqslant n-1$, let $\theta_{i,n}$ be the a-word $\phi_n^{i+1}(\delta_{n-1})$. Then $\theta_{i,n}$ is equivalent to $\delta_n\,\sigma_i^{-1}$, and it has length $n-2$.*

Proof. By Lemma 1.6, we have $\phi_n^{i+1}(a_{n-1,n}) = a_{i,i+1}$. We deduce $\phi_n^{i+1}(\delta_n) \equiv \phi_n^{i+1}(\delta_{n-1})\,\sigma_i = \theta_{i,n}\,\sigma_i$. As δ_n is invariant under ϕ_n, we have $\delta_n = \theta_{i,n}\,\sigma_i$. The length of the a-word δ_{n-1} is $n-2$. As ϕ_n preserves the length of a-word, the length of $\theta_{i,n}$ is $n-2$. □

Proposition 6.4. *For each n-strand braid β, we have $|\beta|_n \leqslant (n-1)\,\|\beta\|_\sigma$. Moreover, if β is specified by a word of length ℓ, the rotating normal form of β can be computed in time $O(\ell^2)$.*

Proof. The case $n = 2$ is trivial. Starting with a word on the alphabet $\{\sigma_1, \sigma_1^{-1}\}$, we freely reduce it to σ_1^k by deleting the factors $\sigma_1\sigma_1^{-1}$ and $\sigma_1^{-1}\sigma_1$. The rotating normal form is $a_{1,2}^k$ in the case $k \geqslant 0$, and $d_{1,2}^k$ in the case $k < 0$, and it is geodesic.

Assume now $n \geqslant 3$. Let w be an n-strand braid word representing β. Then the rotating normal form of β is obtained as follows:

- Replace each positive letter σ_i in w with $a_{i,i+1}$, so as to obtain

$$u = w_0\sigma_{i_1}^{-1}w_1 \ldots w_{c-1}\sigma_{i_{c-1}}^{-1}w_c;$$

- Put $v = \phi_n^c(w_0)\,\phi_n^{c-1}(\theta_{i_1,n}\,w_1)\,\ldots\,\phi_n(\theta_{i_{c-1},n}\,w_{c-1})\,\theta_{i_c,n}\,w_c$;

- Let s be the maximal integer such that δ_n^s left-divides $\overline{v}$ in B_n^{+*}, and let v' be a positive a-word satisfying $v \equiv \delta_n^s v'$;

- If $s \geqslant c$ holds, put $t = 0$ and $w'' = \delta_n^{s-c}\, v'$; otherwise put $t = c - s$ and $w'' = v'$.

- Let w' be the normal form of $\overline{w''}$. Then the rotating normal form of β is $d_{1,n}^{-t}\, w'$.

Indeed, Lemma 6.3 and $\delta_n \equiv d_{1,n}$ imply

$$w \equiv w_0\, d_{1,n}^{-1}\, \theta_{i_1,n}\, w_1 \dots d_{1,n}^{-1}\, \theta_{i_{c-1},n}\, w_{c-1}\, d_{1,n}^{-1}\, \theta_{i_c,n}\, w_c$$

Pushing the letters $d_{1,n}^{-1}$ to the left, we obtain

$$w \equiv d_{1,n}^{-c}\, \phi_n^c(w_0)\, \phi_n^{c-1}(\theta_{i_1,n}\, w_1) \dots \phi_n(\theta_{i_{c-1},n}\, w_{c-1})\, \theta_{i_c,n}\, w_c = d_{1,n}^{-c}\, v.$$

Using the relation $d_{1,n} \equiv \delta_n$ and the construction of w', we obtain $w \equiv d_{1,n}^{-t}\, w'$, where $\overline{w'}$ is not left-divisible by $d_{1,n}$ unless t is zero.

As for the length, replacing σ_{i_k} by $d_{1,n}^{-1}\, \theta_{i_k}$ multiplies it by at most $n-1$. Applying the construction in the case when w is a shortest representative of β gives $|\beta|_n \leqslant (n-1)\|\beta\|_\sigma$.

As for the time complexity, v is obtained in time $O(\ell)$, the integer s is obtained in time $O(\ell^2)$—see for instance [13]—and w' is obtained in time $O(|w''|^2)$ by Proposition 2.13. Hence, as $|w''| \leqslant \ell$ holds, the rotating normal form of β is obtained from the word w in time $O(\ell^2)$. □

Example 6.5. Consider $\beta = \sigma_1\, \sigma_3^{-2}\, \sigma_2\, \sigma_3$. We use the notation of Proposition 6.4. First, we write $u = w_0\, \sigma_3^{-1}\, w_1\, \sigma_3^{-1}\, w_2$ with $w_0 = a_{1,2}$, $w_1 = \varepsilon$ and $w_2 = a_{2,3}\, a_{3,4}$. Then we have $\theta_{3,4} = \phi_4^4(\delta_3) = a_{1,2}\, a_{2,3}$, and we find

$$v = \phi_4^2(w_0)\, \phi_4(\theta_{3,4}\, w_1)\, \theta_{3,4}\, w_2 = a_{3,4}\ \ a_{2,3}\, a_{3,4}\ \ a_{1,2}\, a_{2,3}\, a_{2,3}\, a_{3,4}.$$

The maximal power of δ_4 that left-divides $\overline{v}$ is 1 and we have $v \equiv \delta_4\, a_{2,3}\, a_{1,2}\, a_{2,3}\, a_{2,4}$. So we find $s = 1$ and $v' = a_{2,3}\, a_{1,2}\, a_{2,3}\, a_{2,4}$. Here we have $c = 2$ and $s = 1$ hold, hence we put $t = 1$ and $w'' = a_{2,3}\, a_{1,2}\, a_{2,3}\, a_{2,4}$. The rotating normal form w' of $\overline{w''}$ turns out to be $a_{1,2}\, a_{1,4}\, a_{2,3}\, a_{1,2}$. So, finally, the rotating normal form of β is

$$d_{1,4}^{-1}\, a_{1,2}\, a_{1,4}\, a_{2,3}\, a_{1,2}.$$

Hence the 4-depth of β is 1, its length is 5, and its 4-breadth is 4, since we saw in Example 2.15 that the 4-breadth of $a_{1,2}\, a_{1,4}\, a_{2,3}\, a_{1,2}$ is 4: its ϕ_4-splitting is $(a_{2,3}, a_{2,3}, 1, a_{2,3}\, a_{1,2})$, a sequence of length 4.

6.2. The word $\mathrm{NF}_n(\beta)$: the easy cases.

Starting from the rotating normal form, we shall now define for each braid β a new distinguished representative $\mathrm{NF}_n(\beta)$ that is a σ-definite word. The word $\mathrm{NF}_n(\beta)$ will be constructed as a word on the letters $a_{p,q}$ and $d_{p,q}$. At the end, it will be obvious to translate it into an ordinary braid word, *i.e.*, a word on the letters σ_i.

The construction of $\mathrm{NF}_n(\beta)$ depends on the relative values of $\mathrm{dp}_n(\beta)$ and $\mathrm{br}_n(\beta)$. The first case, which is easy, is when the n-depth of β is 0, *i.e.*, when β belongs to B_n^{+*}, or it is $|\beta|_n$, *i.e.*, when β is a negative power of $d_{1,n}$. Note that this case is the only possible one in the case of B_2.

Definition 6.6. Assume that β is a braid of B_n satisfying $\mathrm{dp}_n(\beta) = 0$ or $\mathrm{dp}_n(\beta) = |\beta|_n$. Then we define $\mathrm{NF}_n(\beta)$ to be the n-rotating normal form of β.

In this case, everything is clear.

Proposition 6.7. *Under the hypotheses of Definition 6.6, the word* $\mathrm{NF}_n(\beta)$ *is a* σ*-definite expression of* β*, and its length is at most* $|\beta|_n$*. Moreover, if* β *is specified by a* σ*-word of length* ℓ*, the word* $\mathrm{NF}_n(\beta)$ *can be computed in time* $O(\ell^2)$*.*

Proof. If $|\beta|_n$ is equal to 0, then β is the trivial braid 1 and its rotating normal form is the empty word. If β is nontrivial with $\mathrm{dp}_n(\beta) = 0$, then the rotating normal form is a nonempty positive a-word, *i.e.*, a σ-positive word. If β is nontrivial with $\mathrm{dp}_n(\beta) = |\beta|_n$, then the rotating normal form of β is $d_{1,n}^{-\mathrm{dp}_n(\beta)}$, which is σ_{n-1}-negative. The complexity statements are clear from Proposition 6.4. □

The second case, which is easy as well, is when the depth is large. We recall that, if w is a normal word, then the ϕ_n-splitting of w is the sequence of normal words that represent the entries in the ϕ_n-splitting of the braid represented by w.

Definition 6.8. Assume that β is a nontrivial braid of B_n with $n \geqslant 3$ satisfying $\mathrm{dp}_n(\beta) \neq 0$ and $\mathrm{dp}_n(\beta) > \mathrm{br}_n(\beta) - 2$. Let $d_{1,n}^{-t}\, w$ be the rotating normal form of β and $(w_b, \dots, w_1)$ be the splitting of w. Then we put

$$\mathrm{NF}_n(\beta) = d_{1,n}^{-t+b-1} \cdot w_b\, d_{1,n}^{-1} \cdot \dots \cdot w_2\, d_{1,n}^{-1} \cdot w_1.$$

Proposition 6.9. *Under the hypotheses of Definition 6.8, the word* $\mathrm{NF}_n(\beta)$ *is a* σ*-negative expression of* β*, and its length is at most* $|\beta|_n$*. Moreover, if* β *is specified by a* σ*-word of length* ℓ*, the word* $\mathrm{NF}_n(\beta)$ *can be computed in time* $O(\ell^2)$*.*

Proof. First, we claim that $\mathrm{NF}_n(\beta)$ is an expression of β. Let $d_{1,n}^{-t}\, w$ be the rotating normal form of β and $(w_b, \dots, w_1)$ be the ϕ_n-splitting of w. We have

$$d_{1,n}^{-t}\, w = d_{1,n}^{-t} \cdot \phi_n^{b-1}(w_b) \cdot \dots \cdot \phi_n(w_2) \cdot w_1. \tag{6.1}$$

Pushing $b-1$ powers of $d_{1,n}$ to the right in (6.1) and dispatching them between the factors w_k, we find

$$\begin{aligned} d_{1,n}^{-t}\, w &= d_{1,n}^{-t} \cdot \phi_n^{b-1}(w_b) \cdot \dots \cdot \phi_n(w_2) \cdot w_1 \\ &= d_{1,n}^{-t+b-1} \cdot d_{1,n}^{-b+1} \cdot \phi_n^{b-1}(w_b) \cdot \dots \cdot \phi_n(w_2) \cdot w_1 \\ &\equiv d_{1,n}^{-t+b-1} \cdot w_b \cdot d_{1,n}^{-1} \cdot d_{1,n}^{-b+2} \cdot \dots \cdot \phi_n(w_2) \cdot w_1 \\ &\equiv \ \dots \ \equiv d_{1,n}^{-t+b-1} \cdot w_b \cdot d_{1,n}^{-1} \cdot \dots \cdot w_2 \cdot d_{1,n}^{-1} \cdot w_1 = \mathrm{NF}_n(\beta). \end{aligned}$$

Next, exactly $\mathrm{dp}_n(\beta)$ powers of $d_{1,n}^{-1}$ occur in $\mathrm{NF}_n(\beta)$. Hence, as $\mathrm{dp}_n(\beta) \neq 0$, at least one $d_{1,n}^{-1}$ appears in $\mathrm{NF}_n(\beta)$. By construction, the intermediate words w_k contain no letter $a_{p,n}$. Therefore, the word $\mathrm{NF}_n(\beta)$ is σ_{n-1}-negative.

As for the length, we find

$$\begin{aligned} |\mathrm{NF}_n(\beta)| &= t - b + 1 + |w_b| + 1 + \dots + |w_2| + 1 + |w_1| \\ &= t - b + 1 + |w| + b - 1 = |d_{1,n}^{-t}\, w'| = |\beta|_n. \end{aligned}$$

Finally, assume that β is specified by a word of length ℓ. Then, by Proposition 6.4, we can compute the rotating normal form of β in at most $O(\ell^2)$ steps. By Lemma 2.14, computing the ϕ_n-splitting of w can be done in $O(|w|)$ steps. Hence, $\mathrm{NF}_n(\beta)$ can be computed in time $O(\ell^2)$. □

6.3. **The word $\mathrm{NF}_n(\beta)$: the difficult case.** There remains the case of a braid β satisfying $\mathrm{dp}_n(\beta) \neq 0$ and $\mathrm{dp}_n(\beta) \leqslant \mathrm{br}_n(\beta) - 2$: this is the difficult case. In this case, it is impossible to directly predict whether β has a σ_{n-1}-positive or a σ_{n-1}-neutral expression, and this is the point where we shall use the ladder and reversing machinery developed in Sections 3, 4 and 5.

Definition 6.10. Assume that β is a nontrivial braid of B_n with $n \geqslant 3$ satisfying $\mathrm{dp}_n(\beta) \neq 0$ and $\mathrm{dp}_n(\beta) \leqslant \mathrm{br}_n(\beta) - 2$. Let $d_{1,n}^{-t}\, w$ be the rotating normal form of β, and $(w_b, \dots, w_1)$ be the ϕ_n-splitting of w. Write $w_{t+2} = w'_{t+2}\, a_{p-1,n-1}$. Put

$$v = \phi_n^{b-1-t}(w_b)\ \dots\ \phi_n^2(w_{t+3})\ \phi_n(w'_{t+2})\ d_{1,p}^{-1}, \quad u_{t+2} = d_{p-1,n-2}^{-1}.$$

Case 1: $w_2 \neq \varepsilon$. Then we put

$$\mathrm{NF}_n(\beta) = v\, w''\, \phi_n(w'_2)\, w_1,$$

where w'' and u_3 are the words produced by Lemma 5.9 applied to the sequence $(w_{t+2}, \dots, w_1)$, the word u_{t+2} and the integer 3, and where w'_2 is the word given by Proposition 5.7 applied to the words w_2 and $\phi_n(u_3)$;
Case 2: $w_2 = \varepsilon$, $w_3 = \dots = w_{k-1} = a_{n-2,n-1}$ and $w_k \neq a_{n-2,n-1}$ for some $k \leqslant t+1$. Then we put

$$\mathrm{NF}_n(\beta) = v\, w''\, \phi_n(w'_k)\, d_{1,n-1}^{-c+2}\, w_1,$$

where w'' and u_{k+1} are the words given by Lemma 5.9 applied to the sequence $(w_{t+2}, \dots, w_1)$, the word u_{t+2} and the integer $k+1$, and where $w'_k\, a_{n-2,n-1}$ is the word produced by Proposition 5.7 applied to the words w_k and $\phi_n(u_{k+1})$;
Case 3: $w_2 = \varepsilon$, $w_3 = \dots = w_{t+1} = a_{n-2,n-1}$ and $v \neq d_{1,n-1}^{-1}$. Then we put

$$\mathrm{NF}_n(\beta) = v\, d_{1,n-1}^{-t+1}\, w_1;$$

Case 4: $w_2 = \varepsilon$, $w_3 = \dots = w_{t+1} = a_{n-2,n-1}$ and $v = d_{1,n-1}^{-1}$. Then we put

$$\mathrm{NF}_n(\beta) = \mathrm{NF}_{n-1}(\delta_{n-1}^{-t}\, \overline{w}_1).$$

Proposition 6.11. *Under the hypotheses of Definition 6.8, the word $\mathrm{NF}_n(\beta)$ is a σ-definite expression of β, and its length is at most $3\,|\beta|_n$. Moreover, if β is specified by a σ-word of length ℓ, the word $\mathrm{NF}_n(\beta)$ can be computed in time $O(\ell^2)$.*

Proof. We use the notation of Definition 6.10. First, we claim that the following equivalence holds:

$$d_{1,n}^{-t}\, w \equiv v\ d_{1,n}^{-t+1}\ \phi_n^{t+1}(u_{t+2})\, \phi_n^t(w_{t+1}) \dots \phi_n(w_2)\, w_1. \tag{6.2}$$

Indeed, as the sequence $(w_b, \dots, w_1)$ is the ϕ_n-splitting of w, we have

$$d_{1,n}^{-t}\, w = d_{1,n}^{-t}\, \phi_n^{b-1}(w_b) \dots \phi_n^{t+1}(w_{t+2}) \dots \phi_n(w_2)\, w_1. \tag{6.3}$$

By construction, w_{t+2} is $w'_{t+2}\, a_{p-1,n-1}$. By (4.1), we have $a_{p-1,n-1} \equiv d_{p-1,n-1}\, u_{t+2}$, hence $w_{t+2} \equiv w'_{t+2}\, d_{p-1,n-1}\, u_{t+2}$. Then, the word $d_{1,n}^{-t}\, w$ is equivalent to

$$d_{1,n}^{-t}\, \phi_n^{b-1}(w_b) \dots \phi_n^{t+1}(w'_{t+2}\, d_{p-1,n-1})\, \phi_n^{t+1}(u_{t+2})\, \phi_n^t(w_{t+1}) \dots \phi_n(w_2)\, w_1. \tag{6.4}$$

We push the factor $d_{1,n}^{-t}$ appearing in (6.4) to the right, until it arrives at the left of the factor $\phi_n^{t+1}(u_{t+2})$. In this way, we obtain

$$d_{1,n}^{-t}\, w \equiv \phi_n^{b-t-1}(w_b) \dots \phi_n(w'_{t+2}\, d_{p-1,n-1})\ d_{1,n}^{-t}\, \phi_n^{t+1}(u_{t+2})\, \phi_n^t(w_{t+1}) \dots \phi_n(w_2)\, w_1.$$

Relation (4.2.i) and (4.2.ii) imply $\phi_n(d_{p-1,n-1})\, d_{1,n}^{-t} \equiv d_{1,p}^{-1}$. Inserting the latter value in the relation above, we obtain (6.2), as expected.

Next, by construction, the word v is σ_{n-1}-nonnegative, and its length satisfies

$$|v| = |w_b| + ... + |w_{t+2}|. \tag{6.5}$$

To go further, we consider the four cases of Definition 6.10 separately. In the first three cases, we shall show that $\mathrm{NF}_n(\beta)$ is σ_{n-1}-positive; in the fourth case, we shall show that $\mathrm{NF}_n(\beta)$ is σ-definite using an induction on n and possibly Propositions 6.7 and 6.9.

Case 1. First, $\mathrm{NF}_n(\beta)$ is equivalent to $d_{1,n}^{-t} w$. Indeed, Lemma 5.9 implies

$$d_{1,n}^{-t}\, w \;\equiv v\, w''\, \phi_n^2(u_3)\, \phi_n(w_2)\, w_1,$$

while Proposition 5.7 implies $\phi_n(u_3)\, w_2 \equiv w_2'$. We deduce

$$d_{1,n}^{-t}\, w \;\equiv v\, w''\, \phi_n(w_2')\, w_1 = \mathrm{NF}_n(\beta).$$

Next, by construction, w_2' is a wall lent on $w_2^{\#}$, hence, by definition, it is σ_{n-2}-positive. So $\phi_n(w_2')$ is σ_{n-1}-positive. As v, w'' and w_1 are σ_{n-1}-nonnegative, $\mathrm{NF}_n(\beta)$ is σ_{n-1}-positive.

As for the length, Lemma 5.9 and Proposition 5.7 imply

$$|w''| \leqslant 3|w_{t+1}| + ... + 3|w_3| - |u_3| - t + 2, \quad |w_2'| \leqslant 3|w_2| + |u_3| - 1.$$

Merging this values with (6.5), and $t > 0$, we deduce $|\mathrm{NF}_n(\beta)| \leqslant 3|w|$.

Case 2. First, we observe that the last letter of w_k must be $a_{n-2,n-1}$: this follows from Corollary 3.11 since, by construction of k, the word w_{k-1} is either ε or $a_{n-2,n-1}$.

Now, we check that $\mathrm{NF}_n(\beta)$ is equivalent to $d_{1,n}^{-t} w$. By Lemma 5.9, we have

$$d_{1,n}^{-t}\, w \;\equiv v\, w''\, d_{1,n}^{-k+2}\, \phi_n^k(u_{k+1})\, \phi_n^{k-1}(w_k)\, \phi_n^{k-2}(a_{n-2,n-1})...\, \phi_n^2(a_{n-2,n-1})\, w_1.$$

By Proposition 5.7, w_k' is a $\phi_n(w_{k+1}^{\#})$-wall and it satisfies $\phi_n(u_{k+1})\, w_k \equiv w_k'\, a_{n-2,n-1}$. Then, we have

$$d_{1,n}^{-t}\, w \;\equiv v\, w''\, d_{1,n}^{-k+2}\, \phi_n^{k-1}(w_k')\, \phi_n^{k-1}(a_{n-2,n-1})\, ...\, \phi_n^2(a_{n-2,n-1})\, w_1. \tag{6.6}$$

Pushing the negative powers of $d_{1,n}$ appearing in (6.6) to the right and dispatching them between the $\phi_n^{\cdot\cdot}(a_{n-2,n-1})$, we find

$$\begin{aligned} d_{1,n}^{-t}\, w \;&\equiv v\, w''\, \phi_n(w_k')\, d_{1,n}^{-k+2}\, \phi_n^{k-1}(a_{n-2,n-1})\, ...\, \phi_n^2(a_{n-2,n-1})\, w_1 \\ &\equiv v\, w''\, \phi_n(w_k')\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1}\, d_{1,n}^{-k+3}\, ...\, \phi_n^2(a_{n-2,n-1})\, w_1 \\ &\equiv \;...\; \equiv v\, w''\, \phi_n(w_k')\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1}\, ...\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1}\, w_1. \end{aligned}$$

Then, $\phi_n(a_{n-2,n-1})\, d_{1,n}^{-1} \equiv d_{1,n-1}^{-1}$ implies

$$d_{1,n}^{-t}\, w \equiv v\, w''\, \phi_n(w_k')\, d_{1,n-1}^{-k+2}\, w_1 = \mathrm{NF}_n(\beta).$$

Next, by construction, w_k' is a $\phi_n(w_{k+1}^{\#})$-wall, hence, by definition, it is σ_{n-2}-positive. So $\phi_n(w_k')$ is σ_{n-1}-positive. As v, w'', and $d_{1,n-1}^{-k+2}\, w_1$, are σ_{n-1}-nonnegative, the word $\mathrm{NF}_n(\beta)$ is σ_{n-1}-positive.

As for the length, Lemma 5.9 and Proposition 5.7 imply

$$|w''| \leqslant 3|w_{t+1}| + ... + 3|w_3| - |u_{k+1}| - t + 2, \quad |w_k'\, a_{n-2,n-1}| \leqslant 3|w_k| + |u_{k+1}| - 1.$$

Merging these values with (6.5) and the hypothesis $t > 0$, we find $|\mathrm{NF}_n(\beta)| \leqslant 3|w|$.

Case 3. As above, we observe that the last letter of w_{t+2} is $a_{n-2,n-1}$, which follows from Corollary 3.11, since w_{t+1} is either 1 or $a_{n-2,n-1}$.

Then, we check that $\mathrm{NF}_n(\beta)$ is equivalent to $d_{1,n}^{-t}\, w$. As the last letter of w_{t+2} is $a_{n-2,n-1}$, the word u_{t+2} is empty. Then, we find

$$d_{1,n}^{-t}\, w \;\equiv v\, d_{1,n}^{-t+1}\, \phi_n^{t}(a_{n-2,n-1}) \,...\, \phi_n^{2}(a_{n-2,n-1})\, \phi_n(\varepsilon)\, w_1. \tag{6.7}$$

Pushing again the negative powers of $d_{1,n}$ of (6.7) to the right and dispatching them between the $\phi_n^{\cdot\cdot}(a_{n-2,n-1})$, we find

$$\begin{aligned} d_{1,n}^{-t}\, w \;&\equiv v\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1}\, d_{1,n}^{-t+2}\, \phi_n^{t-1}(a_{n-2,n-1}) \,...\, \phi_n^{2}(a_{n-2,n-1})\, w_1 \\ &\equiv \;...\; \equiv v\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1} \,...\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1}\, w_1. \end{aligned}$$

Then, $\phi_n(a_{n-2,n-1})\, d_{1,n}^{-1} \equiv d_{1,n-1}^{-1}$ implies

$$d_{1,n}^{-t}\, w \equiv v\, d_{1,n-1}^{-t+1}\, w_1 = \mathrm{NF}_n(\beta)$$

Next, we check that $\mathrm{NF}_n(\beta)$ is σ_{n-1}-positive. As $w_{t+2}^{\#} = a_{n-2,n-1}$ holds, we have

$$v = \phi_n^{b-1-t}(w_b) \;...\; \phi_n^{2}(w_{t+3})\; \phi_n(w_{t+2}'')\; d_{1,n-1}^{-1}$$

By Lemma 3.2(*iii*), if the word w_{t+2}' is not empty, it ends with a letter of the form $a_{\cdot\cdot,n-1}$, hence the word v is σ_{n-1}-positive. Assume that w_{t+2}' is empty and $t \leqslant b-3$ holds. As the word w_{t+2} is $a_{n-2,n-1}$, Corollary 3.11 implies that w_{t+3} ends with $a_{n-2,n-1}$. Then, v ends with $\phi_n^2(a_{n-2,n-1})\, d_{1,n-1}^{-1}$, which is $a_{1,n}\, d_{1,n-1}^{-1}$, hence v is σ_{n-1}-positive.

Relation (6.5) directly implies $|\mathrm{NF}_n(\beta)| = |w|$.

Case 4. By construction, we have $v = d_{1,n-1}^{-1}$. The same analysis as in Case 3 gives $t = b-2$ and

$$d_{1,n}^{-t}\, w \equiv d_{1,n-1}^{-t}\, w_1,$$

The induction hypothesis together with Propositions 6.7 and 6.9 gives $d_{1,n-1}^{-t}\, w_1 \equiv \mathrm{NF}_{n-1}(\delta_{n-1}^{-t}\, \overline{w_1})$, hence $d_{1,n}^{-t}\, w \equiv \mathrm{NF}_n(\beta)$ by definition.

Always by induction hypothesis and Propositions 6.7 and 6.9, we have

$$|\mathrm{NF}_n(\beta)| = |\mathrm{NF}_{n-1}(\delta_{n-1}^{-t}\, \overline{w_1})| \leqslant 3|\delta_{n-1}^{-t}\, \overline{w_1}|_{n-1}.$$

By definition, we have $|\beta|_n = t + |w_b| + ... + |w_1|$ and $|\delta_{n-1}^{-t}\, \overline{w_1}|_{n-1} \leqslant t + |w_1|$, hence $|\delta_{n-1}^{-t}\, \overline{w_1}|_{n-1} \leqslant |\beta|_n$. Then, as we obtain $|\mathrm{NF}_n(\beta)| \leqslant 3|\beta|_n$.

So all cases have been considered, and it only remains to analyze the time complexity. By Proposition 6.4 and Lemma 2.14, the rotating normal form of β and the ϕ_n-splitting of w can be computed in time $O(\ell^2)$. Then, in Cases 1 and 2, Lemma 5.9 is used once for $(w_{t+2}, \dots, w_1)$ and u_{t+2}, with a cost $O(\ell^2)$. In addition, Proposition 5.7 is used at most once with $\phi_n(u_{k+1})$ and w_k ($k = 2$ for Case 1), with a cost at most $O(\max(1, |u_{k+1}|\ell))$. Lemma 5.9 guarantees $|u_{k+1}| \leqslant |u_{k+1}| + t + 1 - c$, *i.e.*, $|u_{t+2}| \leqslant t$. So the total cost entailed by Proposition 5.7 is at most $O(\ell^2)$. The other computations in Cases 1, 2, and 3 require at most $O(\ell)$ steps and, therefore, the total cost of the computation of $\mathrm{NF}_n(\beta)$ is $O(\ell^2)$ in Cases 1, 2 and and 3. The result is similar for Case 4, using the induction hypothesis, and possibly Propositions 6.7 and 6.9. □

6.4. **Putting things together.** Using the σ-definite words $\mathrm{NF}_n(\beta)$ constructed in Sections 6.2 and 6.3, we are now ready to establish Theorems 1 and 2 of the introduction. As a preliminary remark, we observe that the words $\mathrm{NF}_n(\beta)$ do not really depend on the index n.

Lemma 6.12. *If β belongs to B_{n-1}, the words $\mathrm{NF}_n(\beta)$ and $\mathrm{NF}_{n-1}(\beta)$ coincide.*

Proof. An easy verification shows that, if β belongs to B_{n-1}, then either we have $\mathrm{dp}_n(\beta) = 0$ (if β belongs to B^{+*}_{n-1}), or we are in Case 4 of Definition 6.10. In both cases, the definition of $\mathrm{NF}_n(\beta)$ implies $\mathrm{NF}_n(\beta) = \mathrm{NF}_{n-1}(\beta)$. □

So, from now on, we can skip the subscript n and write $\mathrm{NF}(\beta)$ without ambiguity. The main result, of which Theorems 1 and 2 are easy consequences, is as follows. We recall that, for β a braid, $\|\beta\|_\sigma$ denotes the length of the shortest expression of β in terms of the Artin generators σ_i.

Theorem 6.13. *For each n-strand braid β, the ad-word $\mathrm{NF}(\beta)$ is a σ-definite representative of β, and its length is at most $3\,(n-1)\,\|\beta\|_\sigma$. Moreover, if β is specified by a σ-word of length ℓ, the word $\mathrm{NF}(\beta)$ can be computed in time $O(\ell^2)$.*

Proof. Everything is obvious in the case $n = 2$, so we assume $n \geqslant 3$. According to Proposition 6.1, and, according to the case, Proposition 6.7, 6.9, or 6.11, the word $\mathrm{NF}(\beta)$ is, in any case, a σ-definite representative of β, and its length is at most $3|\beta|_n$. On the other hand, Proposition 6.4 implies $|\beta|_n \leqslant (n-1)\|\beta\|_\sigma$, so we deduce the expected upper bound

$$|\mathrm{NF}(\beta)| \leqslant 3(n-1)\|\beta\|_\sigma. \tag{6.8}$$

Finally, gathering the complexity analysis of Propositions 6.4, 6.7, 6.9, and 6.11 shows that, in all cases, $\mathrm{NF}(\beta)$ can be computed in $O(\ell^2)$ steps when β is specified by an initial word of length ℓ. □

As promised, we can now deduce Theorems 1 and 2 in a few words.

Proof of Theorem 1. Let $\underline{\mathrm{NF}}(\beta)$ be the translation of the *ad*-word $\mathrm{NF}(\beta)$ into a σ-word. The formulas of (4.2) show that the translation of a letter $a_{p,q}$ or $d_{p,q}$ with $q \leqslant n$ has length at most $2n-3$. So (6.8) implies $|\underline{\mathrm{NF}}(\beta)| \leqslant 6(n-1)^2\|\beta\|_\sigma$. □

Proof of Theorem 2. Translating $\mathrm{NF}(\beta)$ into $\underline{\mathrm{NF}}(\beta)$ has a linear time cost, so the quadratic upper bound for the computation of $\mathrm{NF}(\beta)$ established in Theorem 6.13 immediately gives a quadratic upper bound for the computation of $\underline{\mathrm{NF}}(\beta)$.

A non-empty σ-definite braid word is never trivial, so computing the word $\mathrm{NF}(\beta)$ solves in particular the word problem of B_n, which is known to have a quadratic complexity exactly for $n \geqslant 3$. Hence the above quadratic upper bound is sharp. □

Let us now give a concrete example of the previous constructions.

Example 6.14. We consider the braid $\beta = \sigma_1\,\sigma_3^{-2}\,\sigma_2\,\sigma_3$ of Example 6.5 again. We saw above that its rotating normal form is the *ad*-word

$$d_{1,4}^{-1}\,a_{1,2}\,a_{1,4}\,a_{2,3}\,a_{1,2}.$$

We saw in Example 2.15 that the ϕ_4-splitting of $a_{1,2}a_{1,4}a_{2,3}a_{1,2}$ is $(w_4, ..., w_1)$, with

$$w_4 = a_{2,3}, \quad w_3 = a_{2,3}, \quad w_2 = \varepsilon, \quad \text{and} \quad w_1 = a_{2,3}a_{1,2}.$$

So we have $\mathrm{dp}_4(\beta) = 1$ and $\mathrm{br}_4(\beta) = 4$, hence $\mathrm{dp}_4(\beta) \leqslant \mathrm{br}_4(\beta)-2$, and we are in the difficult case. With the notation of Definition 6.10, we have $t = 1$ and $w_3 = \varepsilon \cdot a_{2,3}$, so we first put $w'_3 = \varepsilon$, $p = 3$, $v = \phi_4^2(w_4)\,\phi_4(w'_3)\,d_{1,p}^{-1}$, and $u_3 = d_{p-1,2}^{-1}$, *i.e.*, in the current case, $v = a_{1,4}\,d_{1,3}^{-1}$ and $u_3 = \varepsilon$. Then, as we have $w_2 = \varepsilon$, $w_3 = a_{2,3}$ and $v \neq d_{1,3}^{-1}$, we are in Case 3 of Definition 6.10. According to the latter, we define $\mathrm{NF}(\beta) = v\,d_{1,3}^{0}\,w_1$, *i.e.*, $\mathrm{NF}(\beta) = a_{1,4}\,d_{1,3}^{-1}\,a_{2,3}\,a_{1,2}$. This *ad*-word is σ_3-positive: indeed, its σ-translation is the σ-word

$$\underline{\mathrm{NF}}(\beta) = \sigma_1\,\sigma_2\,\sigma_3\,\sigma_2^{-1}\,\sigma_1^{-1}\,\sigma_2^{-1}\,\sigma_1^{-1}\,\sigma_2\,\sigma_1$$

which contains one σ_3, but no σ_3^{-1}, and no $\sigma_i^{\pm 1}$ with $i \geqslant 4$.

In the very simple case of Example 6.14, the reversing machinery is not used (and directly guessing a σ-definite word equivalent to the initial word would have be easy). However, much more complicated phenomena may occur in general, in particular when the braid index reaches 5, which is the smallest value for which there exist ladders with more than one bar. All situations considered in Definition 6.10 may occur when the length and the braid index increase, and explicit examples can easily be found using a computer. The examples witnessing really complicated behaviors, typically requiring more than one reversing step, involve words that are too long to be given here. However their existence confirms the really amazing intricacy of the braid relations.

Acknowledgment

The author wishes to thank Patrick Dehornoy for his help in writing the paper.

References

[1] D. Bessis, *The dual braid monoid*, Ann. Sci. École Norm. Sup. **36** (2003), no. 5, 647–683.

[2] D. Bessis, F. Digne, and J. Michel, *Springer theory in braid groups and the Birman-Ko-Lee monoid*, Pacific J. Math. **205** (2002), no. 2, 287–309.

[3] J. Birman, K.H. Ko, and S.J. Lee, *A new approach to the word and conjugacy problems in the braid groups*, Adv. Math. **139** (1998), no. 2, 322–353.

[4] X. Bressaud, *A normal form for braids*, J. Knot Theory Ramifications **17** (2008), no. 6, 697–732.

[5] S. Burckel, *The wellordering on positive braids*, J. Pure Appl. Algebra **120** (1997), no. 1, 1–17.

[6] P. Dehornoy, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345** (1994), no. 2, 293–304.

[7] ———, *A fast method for comparing braids*, Adv. Math. **125** (1997), no. 2, 200–235.

[8] ———, *Groupes de Garside*, Ann. Sci. École Norm. Sup. **35** (2002), no. 2, 267–306.

[9] ———, *Complete positive group presentations*, J. Algebra **268** (2003), no. 1, 156–197.

[10] ———, *Alternating normal forms for braids and locally Garside monoids*, J. Pure Appl. Algebra **212** (2008), no. 11, 2413–2439.

[11] P. Dehornoy, I. Dynnikov, D. Rolfsen, and B. Wiest, *Ordering braids*, Mathematical Surveys and Monographs, Amer. Math. Soc., in press, 2002.

[12] I. Dynnikov and B. Wiest, *On the complexity of braids*, J. Eur. Math. Soc. **9** (2007), no. 4, 801–840.

[13] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson, and W. Thurston, *Word processing in groups*, Jones & Barlett Publ., 1992.

[14] R. Fenn, M.T. Greene, D. Rolfsen, C. Rourke, and B. Wiest, *Ordering the braid groups*, Pacific J. Math. **191** (1999), no. 1, 49–74.

[15] J. Fromentin, *A well-ordering of dual braid monoids*, C. R. Math. Acad. Sci. Paris **346** (2008), no. 13-14, 729–734.

[16] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford Ser. **20** (1969), 235–254.

[17] T. Ito, *On finite Thurston type orderings of braid groups*, arXiv:math.GR/0810.4074.

[18] D.M. Larue, *Left-distributive and left-distributive idempotent algebras*, Ph.D. thesis, University of Colorado, Boulder, 1994.

Laboratoire de Mathématiques Nicolas Oresme, UMR 6139 CNRS, Université de Caen
BP 5186, 14032 Caen, France

E-mail address: `jean.fromentin@math.unicaen.fr`